Aníbal Manuel da Costa Fernandes

A dimensão política da Segurança para o Ciberespaço na União Europeia:

A Agenda Digital, a Estratégia de Cibersegurança e a cooperação UE-OTAN

Universidade dos Açores

DEPARTAMENTO DE HISTÓRIA,
FILOSOFIA E CIÊNCIAS SOCIAIS

Ponta Delgada

2014

Aníbal Manuel da Costa Fernandes

A dimensão política da Segurança para o Ciberespaço na União Europeia:

A Agenda Digital, a Estratégia de Cibersegurança e a cooperação UE-OTAN

Dissertação Realizada para Obtenção do Grau de Mestre em Relações Internacionais pela Universidade dos Açores (6.º Edição 2012/2014)

Orientadores: **Carlos Eduardo Pacheco Amaral**, Professor Associado com Agregação do Departamento de História, Filosofia e Ciências Sociais da Universidade dos Açores;

António José Telo, Professor Catedrático da Academia Militar da República Portuguesa

Universidade dos Açores

DEPARTAMENTO DE HISTÓRIA,
FILOSOFIA E CIÊNCIAS SOCIAIS

Ponta Delgada

2014

Agradecimentos:

À memória de minha mãe, Francelina, pelos tempos de ausência antes da sua partida a meio desta jornada;

À minha mulher, Cristina, pela paciência e à nossa filha, Carolina, pelas críticas construtivas e apoio de ambas;

Aos meus amigos: Artur Veríssimo, Acir Meirelles e Reinaldo Arruda pelo incentivo e companheirismo;

Aos senhores Professores do Mestrado pelo empenho e aos senhores Orientadores pela disponibilidade;

Aos "motores de busca" na Internet – em particular ao "Dr. Google" (Prof. Doutor Carlos CORDEIRO, 2013) – por ter(em) simplificado esta empreitada;

A todos, o meu muito obrigado.

Índice

Abreviaturas

A/D	Alemanha/Deutchland
ACTA	Anti-Counterfeiting Trrade Agreement
AED/EDA	Agência de Defesa Europeia da UE/European Defence Agency–UE
AFCEA	Associação para as Comunicações e Eletrónica das Forças Armadas–PT
ARPANET	Advanced Research Projects Agency Network
ASEAN	Association of Southeast Asian Nations
BCG	Boston Consulting Group
CA	Canadá/Canada
CCD CoE	Cooperative Cyber Defence Centre of Excellence–NATO
CD&E/CDE	Concept Development and Experimentation
CDC	Cyber Defence Capabilities NATO
CDCSC	Cyber Defense Coordination and Support Centre–NATO
CdE /CoE	Conselho da Europa /Council of Europe
CDMA	Cyber Defence Management Authority–NATO
CDMB	Cyber Defense Management Board–NATO
CE/EC	Comissão Europeia da UE/ European Commission–EU
CEGER	Centro de Gestão da Rede Informática do Governo–PT
CERT	Computer Emergency Response Team–EU (“aka” CSIRT)
Cf.	Conforme
CF.	Confrontar
C-I-A	Confidencialidade, Integridade e Autenticidade/Confidentiality, Integrity and Authenticity
CIGI	Centre for International Governance Innovation–CA
CIWIN	Critical Infrastructure Warning Information Network–EU
CMUE/EUMC	Conselho Militar da UE/European Union Military Committe–EU
CNA	Computer Network Attack/Ataque a Comptadores em Rede
CNCSeg	Centro Nacional de Cibersegurança–PT
CND	Computer Network Defense / Defesa de Computadores em Rede
CNE	Computer Network Exploitation/Espionage/Reconhecimento de Computadores em Rede
CNO	Computer Network Operations
COM	Comunicação em forma Diretiva aos EMs daUE/Communication–EU
CSIRT	Computer Security Incident Response Team - «”aka” de CERT em gíria de Cybersegurança»
CSOC	Cyber Security Operations Centre–UK/GCHQ
C-S-S	Center for Security Studies CH / Centro de Estudos de Segurança do ETH da Suiça
CTAC	Cyber Threat Assessment Cell–NATO
CybCr	Cibercrime / Cybercrime
CySec/CiSeg	Cybersecurity / Cibersegurança
DG CONNECT	DG Communication Networks, Content and Technology EU
DG INFSO	DG Information Society and Media Directorate EU (legacy → DG CONNECT)
DoD	Department of Defense US /Departamento de Defesa EUA
DoS/DDoS	Distributed – Denial of Service
DPA	Data Protection Authority
DPReform	Data Protection Reform–EU
EC3	Centro Europeu de Luta contra o Cibercrime/European Cyber Crime Centre–EUROPOL–EU
ECS/CSS	Estratégia de Cyber Segurança da UE /Cyber Security Strategy–EU
EE	Estonia/Estónia
EEA	European Economic Area–EU
EEE	Equipamento Elétrico e Eletrónico / Electric and Electronic Equipement–EU
EES/ESS	Estratégia Europeia de Segurança da UE /European Security Strategy–EU
EISAS	European Information Sharing and Alert System–EU
EM/ MS	Estado membro / Member State–EU
ENISA	European Network and Information Security Agency–EU
EP3R	European Public Private Partnership for Resilience–EU
EPIC	Electronic Privacy Information Centre–ONG–US
EPPIC	European Program for Critical Infrastructure Protection–EU
ESDP/CSDP	European Security and Defence Policy(formally)/Common Security and Defence Policy–EU
ESI/ISS	Estratégia de Segurança Interna da UE/Internal Security Strategy–EU
eSociety	Information Society in Europe/Sociedade de Informação–EU
ETH	Eidgenössische Technische Hochschule/Swiss Federal Institute of Technology–CH
EUA/USA	Estados Unidos da América/United States of America
EUDRD	European Data Retention Directive–EU
EUISS	European Union Institute for Security Studies
EUROPOL	Polícia Europeia da UE/European Police–EU
F	République Française/República Francesa
FCCN	Federação para a Computação Científica Nacional–PT
FOC	Full Operational Capability–NATO/UK
FR/RF	Federação Russa/Russian Federation
G8	Grupo dos 8 Países com as maiores economias industrializadas
GCHQ	Government Communications HeadquartersUK
GCIG	Global Commission on Internet Governance–CIGI–CA e Chatham House–UK initiative
GDPR	General Data Protection Regulation–EU

GI/IG	Govervação|Governança de Internet/Internet Governance
GNS	Gabinete Nacional de Segurança–PT
GPpI/PSG	Grupo Permanente de partes Interessadas/Permanent Stakeholders Group–ENISA–EU
I&D/R&D	Investigação & Desenvolvimento/Research & Development
IC/CI	Infrastructura Crítica/Critical Infrastructure
IDS	Intrusion Detection System
IEEE	International Electrical and Electronic Engineering
IEFT	Internet Engineering Task Force
IGCI	Global Complex for Innovation INTERPOL
IGF	Internet Governance Forum–ITU-UN
IGP	Internet Governance Project
ISP	Provedores de Serviço/Internet Service Providers
IT/TI	Information Technology/Tecnologias de Informação
ITU	International Telecomunication Union–UN
JAI/JHA	Justiça e Assuntos Internos/Justice and Home Affairs–EU
LEA	Law Enforcement Authorities/Autoridades Judiciais
LIBE	Comissão de Liberdades Civis, Justiça e Assuntos Internos–UE/ Committee on Civil Liberties, Justice and Home Affairs from–EP at EU
LRG	Legislação, Regulamentação e Governança/Legislation, Regulation and Governance
MEP	Membro do Parlamento Europeu da UE /Member of European Parliament – EU
MERCOSUL	Mercado Comum do Sul
MI5	Military Intelligence, Section 5 (United Kingdom's internal counter-intelligence and security agency) UK
MI6	Secret Intelligence, Section 6 UK
MNCD2	Multi National Cyber Defence Capability Development Initiative NATO
MNE	Multinational Experiment
MUD/DSM	Mercado Único Digital/Digital Single Market(legacy →Single European Information Space) –EU
MUE/ESM	Mercado Único Europeu da UE/European Single Market–EU
NAC	Network Analysis Centre–GCHQ–UK
NAC	Conselho de Altântico Norte da OTAN/North Atlantic Council–NATO
NAFTA	North American Free Trade Agreement
NC3A	Consulting, Command and Control Agency–NATO
NCI	Communication and Information Agency–NATO
NCIRC	Computer Incident Response Capability–NATO
NCIRC TC	Computer Incident Response Capability/Technical Center–NATO
NIAG	Industry Assessment Group–NATO
NIS/RSI	Network Information Security/Redes de Sistemas de Informação–EU
NMA	Military Authorities–NATO
NSA	National Security Agency USA/Agência Nacional de Segurança–EUA
OCDE/OEDC	Organização para a Cooperação e Desenvolvimento Económico/Organization for Economic Cooperation and Development
OCSIA	Office of Cyber Security & Information Assurance –GCHQ–UK
OCX/SCO	Organização de Cooperação de Xangai/Schangai Cooperation Organization
OMC/WTO	Organização Mundial do Comércio/World Trade Organization–UN
ONG/NGO	Organizações Não Governamentais/Non Governmental Organizations
ONU/UN	Organização das Nações Unidas/United Nations
OSCE	Organization for Security and co-operation in Europe/Organização p/a Segurança e Cooperação na Europa
OTAN/NATO	Organização do Tratado do Atlântico Norte /North Atlantic Treaty Organization
p.p	Próximo-passado
PB/NL	Baises-Baixos/Nederland
PCPIC	President´s Commission Critical Infrastructure Protection–USA
PCSD/CSDP	Política Comum de Segurança e Defesa/Common Security and Defence Policy (formally, European Security and Defence Policy)–EU
PE/ EP	Parlamento Europeu da UE/European Parliament–EU
PESC/CFSP	Política Externa de Segurança e Defesa da UE/Common Foreign and Security Policy–EU
PIB/GDP	Produto Interno Bruto/Gross Domestic Product
PIC/PIC	Proteção das Infraestruturas Críticas/Critical Infrastruture Protection
PIIC/PICI	Poteção das Infraestruturas Críticas de Informação/Critical Information Infrastruture Protection
PIPA	Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act
PME/SME	Pequenas e Médias Empresas/Small and Medium Enterprises
PPP	Parceria Público Privada/Public Private Partnership
PT	Portugal
q/b	quanto baste
RAND	Nonprofit, nonpartisan, and committed to the public interest research organization
RBN	Russian Business Network-RF
RFB	República Federativa do Brasil
ROI/RdI	Return of Investiment/Retorno do Investimento
RPC/PRC	República Popular da China/People Republic of China
RRT	Rapid Response Team–NATO
RU/UK	Reino Unido da Grã-Bretanha e da Irlanda do Norte/United Kingdom
SCEE	Sistema de Certificação Eletrónica do Estado–PT
SE	Suécia/Sweden
SEAE/EEAS	Serviço Europeu de Ação Externa /European External Action Service–EU

SEGNAC	Segurança de Matérias Classificadas–PT
SI/IS	Sistema de Informação/Information System
SIEM	Security Information Executive Management/Gestão Ececutiva de Segurança da Informação
SOPA	Stop Online Piracy Act
TAO	Tailored Access Operations (NSA)–USA
TdJ/CoJ	Tribunal de Justiça da UE /Court of Justice–EU
TFTP	Terrorist Finance Tracking Program/Programa de Rastreio de Finaciamento ao Terrorismo
TIC/ ICT	Tecnologias de Informação e Comunicação/ Information and Communications Technologies
TTIP	Transatlantic Trade and Investment Partnership/Parceria Trans-atlântica de Comércio e Investimento
UE/EU	União Europeia/European Union
UNGA	United Nations General Assembly–UN
USAF	United states Air Force–USA
VP/AR-VP/HR	Vice-presidente/Alto-representante da UE / Vice-Presidente High Representative– EU
W3C	World Wide Web Consortium
WCIC	World Conference on International Communications–ITU-UN
Wi-Fi	Wireless Fidelity Foundation (tecnologia IEEE 802.11)

Índice de Tabelas e Ilustrações

Abstract

The Cybersecurity is increasingly present in the agendas of many actors and institutions at the political level of the International Community countries and the International Relations (IR) discipline. In the European Union (EU) those problematic issues related to the security field of the fifth domain of geostrategy –Cyberspace– is not recent. The first approach was in 2001 by the European Commission (EC).

These concerns appeared as a result of the emergence of criminal activities through the use of electronic media in the early days of the Internet and the Web and were properly marked by INTERPOL. With the implosion of the Soviet Union and allied countries, the increase of organized crime privileged Cybercrime as preferred mode of operations, due to anonymity and the difficulty of attribution and criminal prosecution, -the insecure nature of cyberspace- and the easy return on "investment" (ROI). It is the Council of Europe (CoE) the first European political institution that detects the situation and work hard in order to frame the issue through a Convention in 2001. The EU introduces the issues of security in their political Agenda to quite the emergence and acceptance of the Convention who "speed-up" the political process.

Associated with the issues of security of electronic crime was the need to increase the use of the Information Society and Knowledge Economy consequent as an instrument of economic growth and the fight against info-exclusion. This strategy was part of the initiatives ***eSociety*** and subsequent ***Action Plans 2002***, ***2005*** and ***2010***.The creation of the European Network Information Security Agency (ENISA), in 2004, was a good decision, because of the need for prospective importance of Cyberspace and the Internet to the EU and to the world. Also with the increase of terrorism in 09/11 (2001) and the Madrid and London attacks which concerns on the Protection of Critical Infrastructure Information, entered the EU Security Agenda.

However, it would be with the events in Estonia in 2007, the EU –among others– that take true awareness of the problem of security in cyberspace. At that time, the EU introduced a positive differentiation among related issues ***eSociety*** and autonomy of subjects related to Networks and Information Systems (NIS) –which means Cybersecurity in the "language" of the EU. Therefore ENISA is no longer a research agency it has been becoming an institution of designing and implementing security solutions for Cyberspace in the EU, the Member States (MSs) and Extra-institutions partners of the EU.

With the entry into force of the EC called "Barroso II", two important EU Cyberspace policy instruments began to be developed: The Digital Agenda and the Cyber Security Strategy (CSS). With regard to this work in particular, relates more specifically with the ***Pillar III of Trust and Security*** of the Digital Agenda and connections of the UE-CSS and Common Foreign and Security Policy (CFSP).

Concerning to this EC, that the European External Action Service (EEAS) by the Treaty of Lisbon, came to have greater responsibilities in defining and implementing actions related to CFSP and the articulation of foreign shares dimension of Common Security and Defence Policy (CSDP) - formally, the European Security and Defence Policy (ESDP).

There are no security mechanisms for Cyberspace and the Internet to be complete and 100% secure, because this is not dichotomous but rather gradual. It is achieved through various vectors of intervention, namely the Resilience, fight for Cybercrime and Deterrence. If ENISA, has worked in the first, will be necessary also to develop mechanisms in the others. The European Cybercrime Center will fight the second. The European Defence Agency (EDA), among others, may contribute also to this effect, leveraging synergies in cooperation with North Atlantic Treaty Organization (NATO), which for several years has been working in that area and they are part of the vast majority MSs of the EU, remaining the rest as partners.

Keywords: ***Cyberspace, Cyber Security, European Union, ENISA, Cyber power, EU- CFSP, EU-CSDP, EU-Digital Agenda, EU-Cyber Security Strategy, NATO***

Resumo

A Cibersegurança é um conceito cada vez mais presente nas agendas dos mais variados atores e instituições ao nível político dos países da Comunidade Internacional e na disciplina de Relações Internacionais (RI). Na União Europeia (UE), a problemática dos assuntos relacionados com a segurança do quinto domínio de geoestratégia –o Ciberespaço– não é recente, datando de 2001.

Essas preocupações surgiram como resultado do aparecimento de ações criminosas através da utilização de meios eletrónicos nos primórdios da Internet e da Web e foram devidamente sinalizadas pela INTERPOL. Com a implosão da União Soviética e países afins, o recrudescimento do crime organizado privilegiou o Cibercrime como modo de operações preferencial, devido ao anonimato e à dificuldade de atribuição e persecução criminal, –pela natureza insegura do Ciberespaço– e ao fácil retorno de investimento (ROI). O Conselho da Europa (CdE) é a primeira instituição política europeia que deteta a situação e trabalha arduamente no sentido de enquadrar o problema através da Convenção em 2001. A UE introduz a problemática da segurança na sua agenda política muito pelo aparecimento e aceitação dessa Convenção, que constituiu um catalisador.

Associado à problemática da segurança do crime eletrónico, estava a necessidade de incrementar a utilização da Sociedade de Informação e a consequente Economia de Conhecimento, como instrumentos de crescimento económico e luta contra a infoexclusão. Esta estratégia inseriu-se nas iniciativas *eSociety* e nos consequentes Planos de Ação de 2002, 2005 e de 2010. A criação da Agência Europeia de Segurança das Redes e da Informação (ENISA), em 2004, foi uma decisão acertada, devido à necessidade prospetiva de importância do Ciberespaço e da Internet para a UE e para o mundo. Também é com o recrudescimento do terrorismo no 09/11 (2001) e dos ataques de Madrid e de Londres que a Proteção das Infraestruturas Críticas de Informação (PIC[I]) entraram nas Agendas de Segurança da UE.

No entanto, seria com os acontecimentos na Estónia (EE) em 2007, que a UE –entre outros– tomava a verdadeira consciência da problemática da segurança no Ciberespaço. Nessa altura, a UE introduz uma diferenciação positiva entre os assuntos relacionados com a *eSociety* e a autonomia de assuntos ligados às Redes e Sistemas de Informação (RSI) –Cibersegurança na "linguagem" da UE. A partir desta altura, a ENISA deixou de ser uma agência de pesquisa, passando a ser uma instituição de conceção e implementação de soluções de segurança para o Ciberespaço na UE, nos Estados Membros (EMs) e com instituições extracomunitárias.

Com a entrada em funções da Comissão Europeia (CE) designada por "Barroso–II", começaram a ser desenvolvidos dois instrumentos importantes para as políticas do Ciberespaço da UE: A Agenda Digital e a Estratégia de Cibersegurança (ECS). Este trabalho é relacionado, mais especificamente, com o seu Pilar III da Confiança e da Segurança, daquela Agenda Digital e com as prioridades da UE-ECS.

É também na vigência da mesma CE, que o Serviço Europeu de Ação Externa (SEAE) pelo Tratado de Lisboa, passou a ter maiores responsabilidades na definição e execução de ações relativas à Política Externa e de Segurança Comum (PESC) e na articulação da dimensão externa de ações da Política Comum de Segurança e Defesa (PCSD)/Política Europeia de Segurança e Defesa (PESD). Não existem mecanismos de segurança para o Ciberespaço e para a Internet completos e 100% seguros, porque aquela não é dicotómica mas sim gradativa. Ela é conseguida através de vários vetores de intervenção, nomeadamente, a Resiliência, combate ao Cibercrime e a Dissuasão. Se a ENISA tem trabalhado na primeira, será necessário desenvolver as outras. O Centro Europeu de Luta contra o Cibercrime (EC3) tentará enfrentar o segundo. Já a Agência Europeia de Defesa (AED) poderá contribuir para, potenciando sinergias, em cooperação com a Organização do Tratado do Atlântico Norte (OTAN), desenvolver a terceira, pois a OTAN há vários anos tem vindo a trabalhar na referida área e a que pertencem a grande maioria dos EMs da UE, sendo os restantes parceiros.

Palavras-chave: ***Ciberespaço, Cibersegurança, União Europeia, ENISA, Ciberpoder, UE-PESC, UE-PCSD, UE-Agenda Digital, UE-Estratégia de Cibersegurança, OTAN***

Introdução

Os primórdios da Cibersegurança na *eSociety* da União Europeia

A Cibersegurança[1], ou Segurança relacionada com o domínio operacional, enquadrado pelo uso da eletrónica para explorar a informação através de sistemas interligados à sua infraestrutura associada ou Ciberespaço[2], presente nas agendas[3] da União Europeia (UE/*European Union–EU*[4]) não é recente[5]. Um documento – considerado relevante, também por (NOTO, 2013, p. 12)– datado do início de 2001,

[1] "Cyber security now clearly comes under the purview of diplomats, foreign policy analysts, the intelligence community, and the military." (CAVELTY M. D., "The militarisation of cyber security as a source of global tension", 2012, p. 112) ou "Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its independent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.[C-I-A]" (HIGH REPRESENTATIVE/VICE PRESIDENT, 2013, p. 3)

[2] Duas definições possíveis e sucintas: "Cyberspace is an operational domain framed by use of electronics to […] exploit information via interconnected systems and their associated infra structure." (NYE Jr., "Cyber Power", 2010, p. 3) citando KUEHL, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem," in KRAMER, Franklin D. – STARR, Stuart and WENTZ, Larry K. eds., *Cyberpower and National Security* (Washington, D.C.: National Defense UP, 2009); ou " [...] a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. " Origin: Cyberspace Operations, Air Force Doctrine Document 3-12, 15 July 2010 pp. 1. Disponível em http://cryptome.org/dodi/AFDD3-12.pdf . Acedido a 11/nov./2012.

[3] "The formation of an agenda may depend on a number of different factors, not least of which are power and politics. This may seem obvious, but, strangely enough, it is perceived as controversial by many in the traditional security studies research community. It has even been claimed that research on how the security policy agenda is set diverts attention away from 'real' problems (KNUNDSEN 2001: 359-61). Security policy researchers rarely hesitate to identify what the real threats are. [...]" (ERIKSSON & NOREEN, 2002, p. 1) citando KNUNDSEN, O. F. (2001) '*Post-Copenhagen Security Studies*', Security Dialogue 32(3): 355-68.

[4] Neste trabalho, as abreviaturas ou acrónimos em itálico estão na Língua original ou em Inglês.

[5] "Like so many other political entities, the European Union has been dialing with cyber-related issues for a number of years [citando (KLIMBURG & TIIRMMA-KLAAR, 2011)] – with varying success." (CAVELTY M. D., "A Resilient Europe for an Open, Safe and Secure Cyberspace", 2013)

indexado por COM(2000) 890[LRG01] [6] e intitulado '*Creating a Safer Information Society by Improving the Security of Information Infrastrutures and Combating Computer-related Crime'*[7], disso atesta. Registe-se, anterior à ocorrência da catástrofe de 11 de setembro (***9/11***). Por isso, não associado à luta "contra o mega terrorismo", mas como consequência do incremento de atividades ilícitas de índole eletrónica, perpetradas pelo crime organizado transnacional nos primeiros anos –1990´s– de Globalização[8]. O corolário mais notório –pela sua sofisticação e amplitude– foi a *Russian Business Network*[9]*–RBN*). Esta, herdou algumas características do estado Soviético e alegadamente manteve ligações informais com os primeiros governos da Federação Russa (FR/*Russia Federation–RF*) (NYE Jr., "Cyber Power", 2010, p. 12). Nesse documento COM(2000) 890[LRG01] a Comissão Europeia (CE/*European Commission–EC*) procurava consubstanciar as suas preocupações e exortava os Estados-membros (EMs/*Member States–MSs*) para alterarem a forma de lidar com o **Internet Crime** ou **Cibercrime**[10] (para mais detalhes sobre a Convenção de Budapeste, visitar o sítio web

[6] O acrónimo LRG refere-se à compilação, não exaustiva, de Legislação, Regulamentação e Governança ou Governação relativos aos temas constantes neste trabalho e poderão ser consultados, como complemento, no Anexo A.i.

[7] COM(2000) 890 final[LRG01]. *"Commission Communication on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime"*. 26 January 2001. Disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF. Acedido a 01/fev./2014. Este documento é também conhecido por *eEurope* action plane 2002.

[8] "[...] le paradigme international qui, depuis les années 1980, avant même la chute du mur de Berlin, et jusqu'au 11 septembre 2001, avait pris le relais du monde bipolaire issu de la guerre froide. Cette période était caractérisée par l'accélération de la mondialisation économique, les progrès planétaires de l'économie de marché et de l'Etat de droit, la révolution technologique, le recul des souverainismes et des tensions géopolitiques, et un leadership occidental incontesté." (COHEN-TANUGI, 2007, p. 31) "[...] the influence of globalisation on the complex interdependence of societies around the world and their growing technological sophistication led to a focus on security problems of a transnational and/or technological nature." (CAVELTY M. D., "The militarisation of cyber security as a source of global tension", 2012, p. 106)

[9] "Organized Crime – One example of organized crime on the web is the Russian Business Network (RBN). The RBN was an Internet service provider [*ISP*] run by criminals for criminals. It is said to have been created in 2004 […] The RBN provided domain names, dedicated servers, and software for criminals on the Internet. […] One example is the infamous Rock Phish scam, in which users were tricked into entering personal banking information on the web, resulting in losses of more than $150 million. The RBN is also said to have provided some support for Russia during its conflicts with Estonia in 2007 and Georgia in 2008." (ROSENZWEIG, 2013, pp. 43 - 44). Para informação complementar, consultar http://www.bizeul.org/files/RBN_study.pdf, consultado a 17/fev./2014.

[10] "The Third INTERPOL Symposium on International Fraud recognized the international feature of computer crime in 1979. But the public awareness about this phenomenon has increased only in the last decade thanks to increased Internet access. The Council of Europe (CoE)[*] and the European Union (EU) are two international organizations most active in the field nowadays. In 2001, CoE released the Convention on Cybercrime[**] and addressed it to all the countries of the world. The EU, instead, turned its reactive approach to the problem into a proactive one rather recently. Initially, the EU concentrated its efforts only responding to cybercrime attacks. Later, it focused on creating a systemic Cybersecurity Strategy to effectively prevent rather than just responding to all kind of attacks. [*] The Council of Europe

do Conselho da Europa [CdE/*Council of Europe–CoE*], em: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185, consultado a 21 de março de 2014). Esta Convenção de 2001 constituiu um "catalisador" para a CE nos assuntos de combate a este tipo de crimes. Instigava os EMs a combater o crime – relacionado com a utilização de computadores em rede– por meios efetivos[11], tendo-se referindo na sua Introdução:

> "Europe's transition to an information society is being marked by profound developments in all aspects of human life: in work, education and leisure, in government, industry and trade. The new information and communication technologies [*ICTs*, ver p. 4] are having a revolutionary and fundamental impact on our economies and societies. The success of the information society is important for Europe's growth, competitiveness and employment opportunities, and has far-reaching economic, social and legal implications." Retirado de COM(2000) 890(LRG01) – 26/jan./2001

Nos dois anos que se seguiram, foram publicados vários documentos da mesma natureza e versando os mesmos temas e preocupações (ver Anexo A.i), sendo três deles significativos: dois definindo e implementando a iniciativa *eEurope 2005*[12] [13]; um outro[14] –considerado relevante na *European Economic Area–EEA*– estabelecendo as

---

is an international organization of 47 states, including also EU MSs. It was created in 1949 in order to promote democracy and protect human rights and the rule of law in Europe. The CoE seat is in Strasbourg, France. **The expression CoE Convention will be also in this work to refer to this document." (NOTO, 2013, p. 2);

[11] "Furthermore, the Communication appears as exhorting the Member States (MSs) to change the way to deal with cybercrime and combat it by effective means." (NOTO, 2013, p. 5)

[12] "The objective of this Action Plan is to provide a favorable environment for private investment and for the creation of new jobs, to boost productivity, to modernise public services, and to give everyone the opportunity to participate in the global information society. *eEurope 2005* therefore aims to stimulate secure services, applications and content based on a widely available broadband infrastructure." Lê-se no Sumário do documento Comission Communication COM(2002) 263 final–*eEurope 2005: Na information society for all* –http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=CELEX:52003XG0228(01):EN:HTML (LRG03). Acedido a 20/fev./2014.

[13] "Council Resolution of 18 February 2003 on the implementation of the *eEurope* 2005 Action Plan(2003/C 48/02) THE COUNCIL OF THE EUROPEAN UNION, Having regard to the Conclusions of the Seville European Council on 21-22 June 2002, Having regard to the *eEurope* 2005 Action Plan presented by the Commission, Having regard to the Conclusions of the Barcelona European Council on 15-16 March 2002, Having regard to the *eEurope* 2002 Action Plan and the " *eEurope* Benchmarking Report *eEurope* 2002" set out in the Commission Communication of 5 February 2002, Having regard to the Commission Communication of 21 November 2002 on " *eEurope* 2005: benchmarking indicators", Lê-se no preâmbulo do documento Council Resolution (2003/C 48/2) (LRG05) *–On the implementation of the eEurope 2005 Action Plan–*, publicado no *Official Journal C 048 , 28/02/2003 P. 0002–0009,* http://eur-lex.europa.eu/LexUriServ/LexUriSrv.do?uri=CELEX:52003XG0228%2801%29:EN:HTML (LRG05). Acedido em 20/fev./2014.

[14] "Regulation (EC) No 460/2004[LRG06] of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance) THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof, Having regard to

bases da Agência Europeia para a Segurança das Redes e da Informação, *European Network and Information Security Agency–ENISA*, ver seção **1.1**. Todavia, foi com a Decisão-Quadro 2005/222/JAI[LRG07] (Justiça e Assuntos Internos–JAI/*Justice and Home Affairs–JHA)* do Conselho de 24 de fevereiro[15] [16] '*On attacks against information systems*', que tinha por objetivo reforçar a cooperação entre as autoridades judiciais (*Law Enfforcement Authorities–LEA*) em matéria dos ataques contra os Sistemas de Informação[17] (SI/*Information Systems–IS*), onde é destacada a preocupação de criar um enquadramento regulamentar ou quadro formal –***Framework***. Estes problemas surgiam, cada vez mais pertinentes, no plano político da UE e suas instituições. Esta problemática era extensível, também, aos EMs com potencial económico e desenvolvimento tecnológico na área das Tecnologias de Informação e Comunicação (TIC/*Information and Communication Technologies–ICT*). Incluíam-se nesse grupo: o Reino Unido (RU/*UK*), a França (F), a Alemanha (A/*D*), a Suécia (SE) a Holanda ou

---

the proposal from the Commission, Having regard to the opinion of the European Economic and Social Committee(1), After consulting the Committee of the Regions, Acting in accordance with the procedure laid down in Article 251 of the Treaty(2), Whereas: (1) Communication networks and information systems have become an essential factor in economic and societal development. Computing and networking are now becoming ubiquitous utilities in the same way as electricity or water supply already are. The security of communication networks and information systems, in particular their availability, is therefore of increasing concern to society not least because of the possibility of problems in key information systems, due to system complexity, accidents, mistakes and attacks, that may have consequences for the physical infrastructures which deliver services critical to the well-being of EU citizens. […]" . Lê-se no preâmbulo do documento Regulation of the European Parliament and the Council (EC) No 460/2004[LRG06] – *Establishing the European Network and Information Security Agency (Text with EEA relevance)* – publicado no *Official Journal L 077 , 13/03/2004 P. 0001 - 0011*, acedido a 20/fev./2014.

[15] Consultado em http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=PT&numdoc=32005F0222&model=guichett [LRG07]. Acedido a 28/jan./2014

[16] Em 30 de setembro de 2010 é apresentada, à CE, uma proposta, por parte do PE e do Conselho, de revogação da Decisão-Quadro 2005/222/JAI[LRG07] indexada Commission Communication COM(2010) 517 Final[LRG29] * *"In June 2011 it was reports that the European Council reached a general approach on the compromise text of the proposed Directive. All EU Member States, with the Exception of Denmark, agreed with this approach. The Directive also refers to 'tools' that can be used in order to commit the crimes listed in the Directive. Examples of such tools include malicious software types that might be used to create botnets. If the offences are against a 'significant' number of computers or affect critical infrastructure then the Directive establishes a minimum sentence of five years. (RAND Europe, 2012, p. 29). Acedido a 08/mar./2014 (Ver Anexo A.i); Ver em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:PT:PDF;

[17] "Qualquer dispositivo ou qualquer grupo de dispositivos interligados ou associados, um ou vários dos quais executem, graças a um programa, o tratamento automático de dados informáticos, bem como dados informáticos por eles armazenados, tratados, recuperados ou transmitidos, tendo em vista o seu funcionamento, utilização, proteção e manutenção." Ver alínea a) do Artigo 1.º da Decisão-Quadro 2005/222/JAI[LRG07].

Países-Baixos (PB/*NL*), que já haviam tomado algumas medidas nesse âmbito[18] [19] (KLIMBURG & TIIRMMA-KLAAR, 2011, pp. 37-39). Nessa "primeira abordagem ou **Fase I**" –da problemática da Cibersegurança– por parte da UE, viria a ser emanado outro documento de enorme importância. Foi indexado por Comission Communication COM(2006) 251 final[LRG11] e intitulado '*Creating a Strategy for a Secure Information Society*'[20]. Na sua introdução foi escrito:

> "The Communication '*i2010* – A European Information Society for growth and employment[i]', highlighted the importance of network and information security for the creation of a single European information space. The availability, reliability and security of networks and information systems are increasingly central to our economies and to the fabric of society. The purpose of the present Communication is to revitalise the European Commission strategy set out in 2001 in the Communication 'Network and Information Security: proposal for a European Policy approach[ii].' It reviews the current state of threats to the security of the Information Society and determines what additional steps should be taken to improve network and information security [RSI/NIS, ver abaixo]. Drawing on the experience acquired by Member States and at European Community level, the ambition is to further develop a dynamic, global strategy in Europe, based on a culture of security and founded on dialogue, partnership and empowerment.[…]"
>
> [i] COM(2005) 229[LRG08] – 01/jun., e [ii] COM(2001) 298[LRG02] – 06/jun.

Após o ano de 2007[21] (iniciava-se uma nova "abordagem ou **Fase II"** –da problemática da Cibersegurança– por parte da UE), denotando-se uma alteração consubstanciada na crescente importância dada à segurança das Redes e Sistemas de Informação (RSI/*Network and Information Systems–NIS*)**,** –sinónimo de

[18] "In 2008 a report on the implementation of 2005/222/JHA was released by European Commission[*]. It concluded that a 'relatively satisfying degree of implementation' had been achieved despite the fact that transposition of the Framework Decision was still not complete. The European Commission invited those seven Member States that, at the time, had not yet communicated their transposition (brought into applicable national law) of the Framework Decision to resolve the issue[**]. Every Member State was asked to review their legislation to better suppress attacks against information systems and the Commission also indicated that given the evolution of cybercrime it was considering new measures as well as promoting the use of the Council of Europe and Group of 8 Nations (G8) network of contact points to react rapidly to threats involving advanced technology. [*] European Commission Report COM (2008) 448; [**]Malta, Poland, Slovakia and Spain did not respond to the request for information and the answers from Ireland, Greece and the United Kingdom were deemed as not possible allow a review of their level of implementation." (RAND Europe, 2012, p. 29)

[19] "It is expected that the Framework Decision on Attacks Against Information Systems 2005/222/JHA will be repealed replaced by a new directive on Attacks Against Information Systems[*], which intends to provide closer harmonisation of the definitions and penalties related to certain types of crimes, and focuses on newer types of cybercrime, such as the use of botnets[TD&T06] (ver Anexo A.ii) as an aggravating circumstance. Additionally, the Directive also aims to strengthen the existing structure of 24/7 national contact points, which should improve and facilitate cross-border communication. [*]For the current draft, seen Council of the European Union, 24/feb./2005." (RAND Europe, 2012, p. 29)

[20] Acedido em http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf. [LRG11] a 28/jan./2014.

[21] "Until 2007, the EU's approach to cyber-security was framed mainly as sub-category and side issue of the efforts to stimulate and secure the development of an Information Society in Europe" (CAVELTY M. D., "A Resilient Europe for an Open, Safe and Secure Cyberspace", 2013, p. 4)

CiberSegurança (CiSeg/*Cybersecurity–CySec)* na "linguagem" da UE[22]–, cada vez mais indissociáveis da Proteção das Infraestruturas Críticas[23] (PIC/*Critical Infrastructure Protection–CIP*), fossem elas de informação (PICI/*Critical Information Infrastruture Protection–CIIP*) ou não, PICs. Era o fim da inclusão das políticas relacionadas com as RSIs, na designada sociedade de informação ou ***eSociety***[24]. Até então, aquelas constituíam uma subcategoria na "visão" da UE. Isso não aconteceu por acaso, sendo consequência de várias razões plasmadas em ambas as "margens" do Atlântico: as consequências do "mega terrorismo" contra as *Twin-Towers* e o "Pentágono" (2001); subsequentes ataques em Madrid (2004) e Londres (2005); a relação com a crescente dependência da sociedade e economia ocidentais na utilização de TICs[25] no Ciberespaço[2] ou Ciberdomínio[26]; a interdependência complexa e estrutural[27] com as Infraestruturas Críticas (IC/*Critical Infrastructures–CI*); e os ataques à Estónia (EE)[28]

---

[22] "Called Network and Information Security (NIS) in EU terminology, cybersecurity […]" (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 31)

[23] "In the contemporary political debate, some objects – commonly called infrastructures – and the functions they perform are regarded as 'critical' by the authorities (in the sense of 'vital', 'crucial', [and] 'essential') because their prolonged unavailability harbours the potential for major crisis, both political and social." (CAVELTY M. D., "A Resilient Europe for an Open, Safe and Secure Cyberspace", 2013, p. 4) citando [BRUGESS, Peter (2007), Social values and material threat: the European Programme for Critical Infrastructure Protection' *International Journal of Critical Infrastructures* 3(3-4): pp. 471-487.]

[24] "Two issues have defined European NIS: firstly, an economic-driven approach to stimulate and secure the development of an Information Society in Europe; secondly, the development of Critical Infrastructure Protection (CIP) as a security issue, originally closed linked to counter terrorism. Officially operating foremost under an 'economic development' mandate, NIS derived in part from the 2005-6 *i2010 initiative* and the European Commission *Strategy for a Secure Information Society* (2006)[(LRG11)] [*'Diálogo, parcerias e maior poder de intervenção'*]." (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 32)

[25] "Virtually all areas of political, economic and social life are today functioning of IT and Internet dependent structures. Business processes between companies rely almost entirely on the Internet as a central infrastructure." Summary from 12/spt./12 of First Cyber Security Summit 2012 in Bonn. Consultado em www.cybersecuritysummit.de a 13/jan./2013.

[26] "The smooth functioning of developed states increasingly relies on assured access to this particular domain." (AALTOLA, SIPILÄ, & VUORISALO, 2011, p. 39); "The main difference between the cyber domain and other global commons is that the cyber domain is entirely a human creation. […] Distance has no meaning in cyberspace. […] There is no space in cyberspace in the spatial sense." (AALTOLA, SIPILÄ, & VUORISALO, 2011, pp. 22 - 23) Para informações complementares sobre *Global Commons* consultar o trabalho de (AALTOLA, SIPILÄ, & VUORISALO, 2011) e para confrontação (CF.) "The cyberspace domain if often described as a public good or a global common, but these terms are an imperfect fit. […] Any cyberspace is not a common like the high seas because parts of it are under sovereign control. At best, it is an 'imperfect commons' […]" (NYE Jr., "Cyber Power", 2010, p. 15)

[27] "[…] Because modern service economies are characterized by complex and network modes of production, these economies require as preconditions both safe Internet-based communications infrastructure […]" (BENDIEK & PORTER, European Cyber Security within a Global Multistakeholder Structure, 2013, p. 164)

[28] "Until 2007, the EU's approach in CIIP was largely constrained to a sub-category of Information Society developments. […] After the 2007 Estonian attacks, DG INFSO raised cybersecurity on the agenda of EU ministers and launched the first EU CIIP policy. Progress in this area has not always seemed to be uniform." (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 31) cf "After the 2007 Estonian attacks[*] the European Commission started to tackle the issue of significant cyber-attacks as a security issue on its own right (European Commission 2009 149 Final[LRG23]), steadily building up a body of directives and Regulations with bearing on cyber-issues. [*]The 2007 Estonia case refers to a series of cyber-attacks on Estonian digital infrastructure in the aftermath of the removal of a statue of a World War II-era Soviet soldier from a park." (CAVELTY M. D., "A Resilient Europe for an Open, Safe and Secure Cyberspace", 2013, p. 4)

(2007). Por norma, nas democracias e economias de mercado, as ICs eram e são geridas através de Parcerias Público-Privadas[29] (PPP/*Public-Private Partnerships–PPP*). Estavam, e continuam, presentes em vastos setores de atividade das ICs e ligadas, nomeadamente: à energia (produção, armazenamento e distribuição); às águas (captação, tratamento e distribuição); à saúde (manutenção e gestão de equipamentos críticos, registo de dados dos pacientes –diagnóstico e pessoais– e administração de prescrições); aos transportes (gestão e manutenção); às finanças (sistemas financeiros, interbancários e de *stocks*); à economia (cadeias de produção[30] e distribuição de produtos e serviços); e, às telecomunicações (fixas, móveis, de voz e dados, de controlo aéreo).

Notas do "*Tio Sam*": As Infraestruturas Críticas e o "*Big – brother"*

As PICs eram preocupações anteriores ao *9/11* (11 de setembro) do outro lado do Atlântico, formalizadas com a iniciativa Presidencial duma Comissão de acompanhamento desse tipo de infraestruturas[31]. Data de 1997, a criação duma Comissão Presidencial de Acompanhamento das ICs –a '***President's Commissionon Critical Infrastructure Protection'–PCPIC,*** ordenada pela Administração CLINTON, após o ato terrorista interno de *Oklahoma City* de 1995. Em 1998, «[…] a mesma Administração publicou um 'Livro Branco' onde emanava uma Política de Proteção das ICs e dava ênfase à proteção das mesmas contra ciberataques.»[32] Como consequência daquele ignóbil acontecimento *–9/11–*, as preocupações relativas às PICs passaram a

[29] "Public-Private Partnerships (PPP), a form of cooperation between the state and the private sector, are widely seen as a panacea for this problem in the policy community – and cooperation programs that follow the PPP idea are part of all existing initiatives in the field of CIP today[*]. [*].Critical infrastructures (CI) are systems or assets so vital to a country that any extended incapacity or destruction of such systems would have a debilitating impact on security, the economy, national public health or safety, or any combination of the above. The most frequently listed examples encompass the sectors of banking and finance, government services, telecommunication and information and communication technologies, emergency rescue services, energy and electricity, health services, transportation, logistics and distribution, and water supply [1, p. 527ff.][*+]. [*+]BRUNNER, Elgin M. and SUTER, Manuel, International CIIP Handbook 2008/2009. *An Inventory of 25 National and 6 International Critical Insfrastructure Protection Policies* (Zurich: CSS, 2008).", citando (CAVELTY & SUTER, "Public-Private Partnership are no silver bullet: An expanded governance model for Critical Infrastructure Protection", 2009, p. 1)

[30] "[…] Secure modes of communication are the prerequisite for organizing the different production phases, for transferring knowledge and for structuring the production chain. A significant proportion of the public infrastructure and services are also connected to the Internet and thus highly vulnerable to cyber attacks." (BENDIEK, "European Cyber Security Policy", 2012, p. 10) baseando-se no trabalho "For an overview of national policies that aim at protecting critical infrastructures, see BRUNNER, Elgin M. and SUTTER, Manuel, International CIIP Handbook 2008/2009. *An Inventory of 25 National and 7 International Critical Insfrastructure Protection Policies* (Zurich: CSS, 2008)."

[31] "In the mid-1990s, the issue of cybersecurity was persuasively interlinked with this topic [*CIP*/PIC] of critical infrastructures and their necessary protection." (CAVELTY M. D., "A Resilient Europe for an Open, Safe and Secure Cyberspace", 2013, p. 4), fazendo referência à PCCIP President's Commission on Critical Infrastructure Protection (1997) *Critical Foundations: Protecting America's Infrastructures*, Washington: US Government Printing Office.

[32] "[…] the CLINTON administration published a White Paper outlining the Policy on Critical Infrstructure Protection and enphazing the importance of protecting critical infrastructure from cyber attacks." (LAASME, 2012, p. 15).

ocupar uma posição estratégica na Administração BUSH, após o mesmo. O interesse funcional e transversal das ICs na Sociedade Norte-americana (confirmado, posteriormente, pelo interesse superior da sua inclusão na agenda política de Washington, pelas Administrações OBAMA[33]) era partilhado pela necessidade psicológica da segurança coletiva (por vezes exacerbada[34] e aproveitada, abusivamente, para permitir outros objetivos –programas sob o controlo dos Serviços de Inteligência. Todas estas ações serviram de suporte à «projeção de *softpower* ["poder suave"][35]» (GEERS, 2013, p. 2). Nessa tónica, sob o pretexto da designada «Guerra contra o Terror[ismo] e o 'Eixo-do-mal' [Irão, Coreia do Norte, Cuba, etc.]» (BUSH, George W., 2001), foram criados programas de controlo de entradas/saídas e de permanência de cidadãos estrangeiros. Foram, de igual modo, implementados sistemas de rastreio de tráfego de entrada nos organismos federais através de vários programas, como por exemplo, o **Einstein** (que se encontra, provavelmente, na sua versão 4.0), estando devidamente preparado para monitorizar, também, o setor privado[36], bastando que estes atores privados o queiram ou, de forma tácita o "autorizem" –esta autorização seria uma consequência de coação na futura exclusão de contratos federais, nomeadamente nas áreas da segurança e da defesa –invocando a «cadeia de produção»[28]. Aqueles sistemas de rastreio, tudo indicava, interferiram com os direitos civis inscritos, em particular, no *Fourth Amendement*[37] da Constituição Americana[38]. Era feito através da interceção

[33] "Cyberspace, and the technologies that enable it, allow people of every nationality, race, faith, and point of view to communicate, cooperate, and prosper like never before. […] Cyberspace is not an end unto itself; it is instead an obligation that our governments and societies must take on willingly, to ensure that innovation continues to flourish, drive markets, and improve lives. […] In this spirit, I offer the United States' International Strategy for Cyberspace. […] And so this strategy outlines not only a vision for the future of cyberspace, but an agenda for realizing it. […]" (THE WHITE HOUSE, 2011)

[34] "These trends have occasioned US officials to frequently talk about the growing potential for a 'Cyber 9/11' or 'Cyber Pearl Harbor'. The purpose of the references is to both highlight the damage that a cyber attack could cause in the physical world and to prepare the population for such an attack. The shrill tone of the warnings also reflects a particular American sense of vulnerability which is not always based on reality." (SALONIOUS-PASTERNAK & LIMMÉIL, 2012, p. 3)

[35] "In 1990, I distinguished hard and soft power along a spectrum from command to co-optive behavior. Hard power behavior rests on coercion and payment. Soft power behavior rests on framing agendas, attraction or persuasion." (NYE Jr., "Cyber Power", 2010, p. 2); "Soft power can rest on the appeal of one's ideas or culture or the shape the preferences of others. […]" (KEOHANE & NYE JR., 1998, p. 86)

[36] "These private networks are the same ones we all use in our online activities. Einstein 2.0 operates through a 'look-up' system. It has a database of known malicious code signatures and constantly compares incoming messages with that database. When it finds a match, it sends an alert to the recipient. These malicious signatures are gathered from a variety of sources, including both commercial firms, such as Symantec, and government agencies, such as the National Security Agency (NSA). Einstein 2.0 is a gateway system; it screens but does not stop traffic as it arrives at federal portals. Einstein 3.0, the next generation of the program, is based on a classified NSA program known as Tutelage and is different in several respects. […] There is little legal debate over the operation of [deste tipo de programas] Einstein 3.0 as applied to government networks. Almost everyone who has examined the question agrees that it is appropriate and necessary for the government to monitor traffic to and from its own computers. Legal disagreement is much more likely to arise over how deeply a government-owned and –operated system may be inserted into private networks, to protect either the government or private-sector users. Would such a system pass constitutional muster?" (ROSENZWEIG, 2013, pp. 80-81)

[37] "Current doctrine makes it clear that there is a difference in the level of constitutional protection between the content of a message and the non-content portions, such as the address on the outside of an

abusiva de comunicações eletrónicas de e para os EUA, ou que "passassem" pelo território norte-americano –i.e. nas "camadas" inferiores[39] do Ciberespaço sob jurisdição americana[40], «as práticas de vigilância eram/[são] um outro exemplo do império da informação: o programa[45] PRISM acede a dados dos utilizadores no Skype e Microsoft, Google, Facebook, AOL, Apple, e outros[41],» (LOSEY, 2014, pp. 85-86) incluindo as infraestruturas de empresas multinacionais a operar, por exemplo na Europa, em particular na Irlanda (ver Seção **1.5**, p.75)–, fossem elas de voz, imagem ou dados com preponderância para aquelas transmissões que utilizavam a Internet[42]. Todos

---

envelope. In general, the non-content portions of intercepted traffic are not protected by the Fourth Amendment, which prohibits unreasonable searches and seizures." (ROSENZWEIG, 2013, p. 81)

[38] " […] During his deliberations, OBAMA has had to reconcile his duties as a commander-in-chief sworn to keep Americans safe and his oath to uphold the US Constitution. […]" Consultado em http://www.nst.com.my/business/nation/obama-to-unveil-nsa-reforms-response-to-snowden-1.464420 a 28/mai./2014.

[39] "In practice, governments and geographical jurisdictions play a major role, but the domain is also marked by power diffusion. One can conceptualize cyberspace in terms of many layers of activities, but a simple first approximation portrays it as a unique hybrid regime of physical and virtual properties.* The physical infrastructure layer follows the economic laws of rival resources and increasing marginal costs, and the political laws of sovereign jurisdiction and control. The virtual or informational layer has economic network characteristics of increasing returns to scale, and political practices that make jurisdictional control difficult.** *LIBICKI distinguishes three layers: physical, syntactic and semantic. See LIBICKI, Martin, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND, 2009), 12. However, with applications added upon applications, the internet can be conceived in multiple layers. See BLUMENTHAL, Marjory and CLARK, David D., "The Future of the Internet and Cyberpower," in KRAMER, cited." (NYE Jr., "Cyber Power", 2010, p. 3) CF. com "At the bottom is the "geographic layer," that is, the physical location of elements of the network. Though cyberspace itself has no physical existence, every piece of equipment that creates it is physically located somewhere in the world. As a consequence, the physical pieces of the network are subject to the control of many different political and legal systems. Next is the "physical network layer"— the hardware and infrastructure of cyberspace, all of which is connected. The components we think of in this layer include all the wires, fiber- optic cables, routers, servers, and computers linked together across geographic spaces. To be sure, some of the links are through wireless connections, but all of those connections have physical endpoints. Above these two real-world layers is the logic layer that we've already described. This is the heart of the network, where the information resides and is transmitted and routed. Above the logic network layer is the "cyber persona layer," which includes such things as a user's e-mail address, computer IP address, or cell phone number. Most individuals have many different cyber personae. Finally, at the top, there is the "personal layer," which encompasses the actual people using the network. Just as an individual can have multiple cyber personae, a single cyber persona can have multiple users, and it is often difficult to link an artificial cyber persona to a particular individual. The true maliciousness of the network comes to the fore at this level, where people choose to act in malevolent ways. " (ROSENZWEIG, 2013, pp. 15-16)

[40] "In this essay, I argue that we can observe in international politics today a simultaneous double move: the territorialisation of cyberspace and the deterritorialisation of state security." (HERRERA, 2007, p. 68)

[41] "[…] and states seeking extraterritorial control of content or access to data." (LOSEY, 2014, p. 85) e "extraterritorial applications of internet jurisdiction […] US surveillance practices are another example of information empire: the PRISM program accesses user data from Skipe and Microsoft, Google, Facebook, AOL, Apple, and others.* * GREENWALD, Glenn and MACASKILL, Ewen, '*NSA Prism Program taps in to user data of Apple, Google and others*,'" The Guradian, June 7, 2013, Accessed July 10, 2014, http://theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. " (LOSEY, 2014, p. 86)

[42] "Well not exactly everyone because the U.S. intelligence only has a legal right to monitor foreigners. They can monitor foreigners when foreigners' data connections end up in the United States or pass through the United States. And monitoring foreigners doesn't sound too bad until you realize that I'm a foreigner and you're a foreigner. In fact, 96 percent of the Planet are foreigners." (HYPÖNNEN, 2013, p. 3':17") Consultado a 11/nov./2013, em http://www.ted.com/talks/mikko_hypponen_how_the_nsa_betrayed_the_world_s_trust_time_to_act#t-752203

estes "atropelos" às liberdades civis foram sendo feitos, à revelia ou com a conivência, igualmente, das Administrações OBAMA, até ao Verão passado, sob pretexto de proteção das PICs[43] em relação ao "mega terrorismo". Foi quando "extrapolou" para a opinião pública o escândalo da *massive surveilance*[44] –implementada pela Agência de Segurança Nacional dos EUA (*National Security Agency–NSA*) através de vários programas, até então, classificados[45]– , trazido para a opinião pública, a 6 de junho de 2013, pelo antigo trabalhador, de um contratante do Departamento de Defesa (DdD/*Department of Defence–DoD*), Edward Snowden, atualmente com autorização de residência temporária renovada, após um ano –notícia da renovação em http://www.breakingnews.com/item/2014/08/07/breaking-former-nsa-contractor-edwardsnowden-ha/ , consultado a 2 de setembro de 2014–, na FR, "oferecida" pelo governo do Presidente Vladimir Vladimirovich PUTIN.

Do lado de cá do Atlântico, estes acontecimentos de "escutas generalizadas", indiscriminadas e continuadas de cidadãos e, até de líderes políticos europeus, e não só, –como as, supostas, violações de mensagens de correio eletrónico efetuadas ao presidente dos Estados Unidos Mexicanos, vizinho e membro do *North American Free Trade Agreement*/*NAFTA*, e à Presidente da República Federativa do Brasil–RFB, etc.–, às instituições da UE[46] e/ou suas representações nas Nações Unidas (ONU/*United Nations–UN*) e na própria Europa, incluindo os EMs (i.e. a Alemanha). Estas revelações

[43] "Federal programs, for on-network monitoring go by the generic name Einstein. Einstein 2.0 is an intrusion detection system [*IDS*] fully deployed by the federal government in 2008 to protect federal cyber networks. A later iteration of Einstein will be moved from the federal system and deployed on private networks to protect critical infrastructure [*CIP*]." (ROSENZWEIG, 2013, p. 80)

[44] "So it is wholesale blanket surveillance of all of us, all of us who use telecommunications and the Internet." (HYPÖNNEN, 2013, p. 3':48")

[45] "So the four main arguments supporting surveillance like this, well, the first of all is that whenever you start discussing about these revelations, there will be naysayers trying to minimize the importance of these revelations, saying that we knew all this already, we knew it was happening, there's nothing new here. And that's not true. Don't let anybody tell you that we knew this already, because we did not know this already. Our worst fears might have been something like this, but we didn't know this was happening. Now we know for a fact it is happening. We didn't know about this. We didn't know about PRISM. We didn't know about XKeyscore. We didn't know about Cybertrans. We didn't know about DoubleArrow. We did not know about Skywriter -- all these different programs run by U.S. intelligence agencies. But now we do." (HYPÖNNEN, 2013, p. 4':45")

[46] "And then the argument that the United States is only fighting terrorists. It's the war on terror. You shouldn't worry about it. Well, it's not the war on terror. Yes, part of it is war on terror, and yes, there are terrorists, and they do kill and maim, and we should fight them, but we know through these leaks that they have used the same techniques to listen to phone calls of European leaders, to tap the email of Presidents of Mexico and Brazil, to read email traffic inside the United Nations Headquarters and E.U. Parliament, and I don't think they are trying to find terrorists from inside the E.U. Parliament, right? It's not the war on terror. Part of it might be, and there are terrorists, but are we really thinking about terrorists as such an existential threat that we are willing to do anything at all to fight them? Are the Americans ready to throw away the Constitution and throw it in the trash just because there are terrorists? And the same thing with the Bill of Rights and all the amendments and the Universal Declaration of Human Rights and the E.U. conventions on human rights and fundamental freedoms and the press freedom? Do we really think terrorism is such an existential threat, we are ready to do anything at all?" (HYPÖNNEN, 2013, p. 12':35") Consultado a 11/nov./2013, em http://www.ted.com/talks/mikko_hypponen_how_the_nsa_betrayed_the_world_s_trust_time_to_act/transcript

constituíram uma imensa surpresa e provocaram um agastado mal-estar entre os representantes políticos de países, supostamente, "amigos" e também aliados na Organização do Tratado do Atlântico Norte (OTAN/*North Atlantic Treaty Organization–NATO*). Esta surpresa foi ainda maior quando, após os ataques ao *World Trade Center* (1993) e o *9/11*, havia sido dada pelos mesmos países europeus toda a colaboração solicitada pelos EUA, incluindo, a transferência de dados significativos de cidadãos europeus e de transações financeiras (*Terrorist Finance Tracking Program–TFTP*), de forma automática[47] e associada à ***European Data Retention Directive–EUDRD***, recentemente, rejeitada pelo Tribunal de Justiça da UE[48] (TdJ/*Court of Justice–CoJ*) (Ver seção **1.5. Os Direitos dos Cidadãos, a Privacidade e a Proteção de Dados**). Apesar do que dizíamos –do lado de cá do Atlântico–, se calhar, deveríamos excluir o *UK*, porque os serviços de inteligência britânicos, através do *Government Communications Headquarters–GCHQ* estiveram, sugestivamente, "mais informados" sobre as atividades da *NSA* do que os serviços dos restantes países europeus "amigos" e aliados na OTAN. Sugestivamente, por participarem na suposta rede de escuta planetária conhecida por ***ECHELON***[49]–que, alegadamente, conta(va) com a participação de outros países da Commonwealth, como o Canadá–Ca, a Austrália–Au e Nova-Zelândia–NZ, também conhecidos por *Five Eyes*, desde a II Guerra-Mundial. O ***ECHELON***, de igual forma, supostamente, poderia alimentar as "escutas" processadas e armazenadas pela Agência Nacional de Segurança/*National Segurity Agency–NSA*, em território americano. Esta situação, levou à indignação geral nos EMs da UE, conduzindo, mesmo, ao "esfriamento" das relações transatlânticas, à ameaça da suspensão das negociações do *Transatlantic Trade and Investiment Partnership–TTIP* e à propalada ausência do Presidente americano na cimeira da Primavera p.p./próximo-passado, em Bruxelas –que acabou por não acontecer, devido à precipitação da situação

---

[47] "- Tendo em conta os acordos entre os Estados Unidos da América e a União europeia sobre a utilização e transferência dos dados contidos nos registos de identificação dos passageiros (Acordos PNR), de 2004, 2007* e 2012**," *JO L204 de 4/ago./2007, p.18 e ** JO L215 de 11/ago./2008, p.5. (MORAES, Claude, 2014, p. 5)

[48] "The Court of Justice ("CoJ") of the European Union ("EU") has declared the Data Retention Directive 2006/24/EC ("Directive") to be invalid (the "Decision"). We provide for a summary of the Decision and discuss its possible consequences, including reactions to the judgment in Germany, the United Kingdom, France, Italy, Spain, the Netherlands and Belgium. […](Press release of the Court of Justice available under http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf) Full text of the Decision available under http://curia.europa.eu/juris/documents.jsf?num=C-293/12.)" em http://www.mondaq.com/x/306158/Data+Protection+Privacy/EU+Data+Retention+Directive+declared+null; consultado a 19/abr./2014.

[49] "Tendo em conta as suas resoluções, de 5 de setembro de 2001 e de 7 de novembro de 2002, sobre a existência de um sistema mundial de interceção das comunicações privadas e comerciais (sistema de interceção ECHELON), […]" (MORAES, Claude, 2014, p. 7) ;"Na sequência da Resolução do Parlamento Europeu, de 4 de junho de 2013 (n.º 16), a CE LIBE realizou uma série de audições para recolher informações relacionadas com os diferentes aspetos em causa, avaliar o impacto das atividades de vigilância em questão, […] 5 de setembro de 2013 15h00-18h30 (BLX); Objeto: Acompanhamento da CE Temporária sobre o Sistema de Interceção ECHELON; Especialistas: Carlos COELHO (deputado ao Parlamento Europeu), antigo presidente da CE Temporária sobre o Sistema de Interceção ECHELON, Gerhard SCHMID (ex-deputado ao Parlamento Europeu), e relator do relatório sobre o ECHELON, de 2001) […]" (MORAES, Claude, 2014, p. 58)

na Ucrânia, gerada pela estratégia do Presidente da FR, recentemente conotado como «Czar de todas as Rússias»[50] (GASTON-ASH, Timothy).

Fez, também, com que e o Parlamento Europeu (PE/*European Parliament–EP)* conduzisse um inquérito que terminou, recentemente, (cujas reações em plenário não foram unânimes[51]) – indexado por **A7-0139/2014**[LRG108] e designado '*US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens´ fundamental rights'* (ver as seções **1.2. O Pilar III de Confiança e Segurança** da Ageanda Digital **1.5. Os Direitos dos Cidadãos, a Privacidade e a Proteção de Dados**). O relator foi, precisamente, um euro-parlamentar britânico, oriundo da região metropolitana de Londres: Claude MORAES[52] da Comissão de Liberdades Civis, Justiça e Assuntos Internos–*LIBE*. Estes acontecimentos –do lado de cá e de lá do Atlântico– "obrigaram" a Administração OBAMA a efetuar algumas alterações de procedimentos, de protocolos no funcionamento e de chefias na *NSA*[53] [54].

---

[50] Artigo "*Putin's Deadly Doctrine 'Protecting' Russians in Ukraine Has Fatal Consequences",* em http://www.nytimes.com/2014/07/20/opinion/sunday/protecting-russians-in-ukraine-has-deadly-consequences.html?ref=opinion&_r=2, consultado em 23/jul./2014.

[51] "First of all, a big tank you to the rapporteur Claude MORAES and their great job and the fellows shadow rapporteures on the match, The very proud that the only Parliament, the only Parliament and the only institution in Europe that has raced this issue, with very limited means, we conducted the inquiry, where the Councilor has been shame fully silent, they has not even them put officially on the agenda of the Council. Massive violation of the rights of the European Citizens has been ignored by the Council. Shame on you! […]Why not opposition politicians? They want to stop then. They even listening, not only, to the mobile phone of Mrs. MERKEL or Mr. HOLLAND, even Mrs. [Dianne] FEINSTEIN [D-CA-California, Head of Senate Intelligence Committee]. How means far this will go? How can be sure that is not the very fabric of our democracy, the rule of law that we are talking about and a fined unbelievable that the European Popular Party (EPP) still hesitations here and ECR [*European Conservatives and Reformists Group* no *EP*.] Is actually gone to vote against. This House was a standard for the right of European citizens, for democracy, for the rule of law. The way is late out our treaties. That is our job!" *Sophie in 't VELD 11 Mar 2014 plenary speech on Report: Claude MORAES (A7-0139/2014) – US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights* em http://www.vieuws.eu/alde/alde-sophie-in-t-veld-on-us-nsa-surveillance-programme/;Consultado a 02/abr./2014.

[52] "Claude MORAES [S&D] is the lead rapporteur of the Committee on Civil Liberties, Justice and Home Affairs (LIBE) inquiry into the NSA spying scandal and its implications on European citizens. In this interview MORAES discusses what impact the inquiry will have on EU citizens and the business community. 'We hope that this inquiry will bring us a step forward in data protection and regulation legislation', argues MORAES. According to the leading MEP, the inquiry calls to rethink the meaning of privacy and surveillance: 'We hope that a proper balance between data gathering and security will be reached'." Em entrevista dada à jornalista Jennifer BAKER em 13/fev./2014 consutada em http://www.vieuws.eu/ict/nsa-scandal-reinforces-the-need-for-data-protection-reform-argues-lead-mep-moraes/ a 28/fev./2014.

[53] "The director of the U.S. National Security Agency and his deputy are expected to depart in the coming months, U.S. officials said on Wednesday, in a development that could give President Barack OBAMA a chance to reshape the eavesdropping agency. Army General Keith ALEXANDER's eight-year tenure was rocked this year by revelations contained in documents leaked by former NSA contractor Edward SNOWDEN about the agency's widespread scooping up of telephone, email and social-media data. ALEXANDER has formalized plans to leave by next March or April, while his civilian deputy, John "Chris" INGLIS, is due to retire by year's end, according to U.S. officials who spoke on condition of anonymity." Consultado em http://www.reuters.com/article/2013/10/16/us-usa-nsa-transition-idUSBRE99F12W20131016 a 28/mai./2014 CF. "GEN Keith ALEXANDER – Commander, U.S. Cyber Command/Director, NSA/Chief, CSS – is pleased to announce that Richard "Rick" LEDGETT is now the 15th Deputy Director of the National Security Agency. In his new role as the senior civilian at NSA,

Estes episódios, poderão estar já a condicionar, a postura da UE na sua relação bilateral com os EUA, –ou não: Possível suspensão do acordo *TFTP*[55], implicações no plano do Grupo de Trabalho UE-EUA sobre a Cibersegurança e o Cibercrime (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 33) e adiamento na conclusão das negociações sobre o futuro acordo, *TTIP*. Poderão, ainda, levar a fricções inevitáveis a nível multilateral dos EMs nos planos da Política de Segurança Interna, Justiça e Direitos Civis com repercussões entre a UE e aqueles ao nível da Política Comum de Segurança e Defesa[56] (PCSD/*Common Security and Defence Policy–CSDP*, [formalmente, *The European Security and Defence Policy–ESDP*]), cada vez mais interligada com a anterior do *DG JUSTICE*, em particular nos assuntos da Cibersegurança[57]. No plano externo, a atuação

---

LEDGETT acts as the agency's chief operating officer – guiding strategies, setting internal policies, and serving as the principal adviser to the Director." Consultado em http://www.nsa.gov/public_info/press_room/2014/new_deputy_director_rick_ledgett.shtml . a 28/mai./2014 e "[…] Mr. Richard (Rick) LEDGETT serves as the Deputy Director and senior civilian leader of the National Security Agency. In this capacity he acts as the Agency's chief operating officer, responsible for guiding and directing studies, operations and policy. He led the NSA Media Leaks Task Force from June 2013 to January 2014, and was responsible for integrating and overseeing the totality of NSA's efforts surrounding the unauthorized disclosures of classified information by a former NSA affiliate. […]" consultado em http://www.nsa.gov/about/leadership/bio_ledgett.shtml e "Admiral ROGERS is a native of Chicago and attended Auburn University, graduating in 1981 and receiving his commission via the Naval Reserve Officers Training Corps. Originally a surface warfare officer (SWO), he was selected for re-designation to cryptology (now Information Warfare) in 1986. He assumed his present duties as Commander, U.S. Cyber Command and Director, National Security Agency/Chief, Central Security Service in April 2014. Since becoming a flag officer in 2007, ROGERS has also served as the director for Intelligence for both the Joint Chiefs of Staff and U.S. Pacific Command, and most recently as Commander, U.S. Fleet Cyber Command/U.S. TENTH Fleet." Consultado em http://www.nsa.gov/about/leadership/bio_rogers.shtml a partir de http://www.nsa.gov/about/leadership/ a 28/mai./2014.

[54] "[…] I want to say a word about the President OBAMA speech last Friday which I think is one significant area signal change in direction is positive. The first key point is that indicated at least the respect in the US that he would and the NSA telephone record collective program and for us in US that has absolutely critical, as we cannot imagine anything worst than an intelligence agency routinely collecting telephone records of all of this citizens. We will work to stop them as President has announced on Friday. […]" aos 44':07" Mr. Marc ROTENBERG of the Electronic Privacy Information Center (EPIC) organization in Washington DC. 7th International Conference – 22, 23 and 24 January 2014, Brussels, Belgium - Computers, Privacy and Data Protection - Reforming Data Protection: The Global Perspective, CPDP 2014: EU Data Protection Reform: State Of Play, que pode ser obtida em https://www.youtube.com/watch?v=kl8an9Myrek; Consultada em 08/ago./2014.

[55] "Tendo em conta a sua resolução, de 23 de outubro de 2013, sobre a suspensão do Acordo [Terrorist Finance Tracking Program] TFTP em consequência da vigilância exercida pela Agência Nacional de Segurança dos EUA;" (MORAES, Claude, 2014, p. 7); "Ação 4: suspender o Acordo TFTP até que (i) tenham sido concluídas as negociações sobre o acordo global; (ii) tenha sido concluído um inquérito aprofundado com base numa análise da UE, e todas as preocupações levantadas pelo Parlamento na sua resolução de 23 de outubro tenham sido devidamente abordadas;" (MORAES, Claude, 2014, p. 48)

[56] "Sendo parte integrante da Política Externa de Segurança e Defesa (PESC/*Common Foreign and Security Policy – CFSP*), a PCSD compreende uma dimensão externa das relações externas da UE estendendo-se para além da dimensão da defesa militar. Sendo uma política sectorial da União e não uma estrutura de defesa, desenvolve-se no âmbito alargado da política externa da UE e comporta uma singular dimensão civil da segurança, que importa desenvolver e integrar no quadro de uma estratégia nacional de participação em compromissos internacionais e nas organizações de que Portugal é Estado membro." (NUNES, 2012, p. 1)

[57] "*The blurring of the boundaries between internal and external policies*: In the area of cyber security, it is almost impossible to maintain the traditional division into internal and external policies. Internet-based attacks can originate in Ghana, Russia or right next door, and it is often difficult (if not impossible) to

tácita de algumas das instituições da UE e de alguns EMs –de maior passividade– perante o tipo de situações relatadas acima, poderão contribuir para aumentar a desconfiança nos fóruns de Governação|*Governança* de Internet (GI/*Internet Governance–IG*, nomeadamente, no *Internet Governance Forum–IGF* da *International Telecommunication Union–ITU* da ONU, etc.. Estas desconfianças poderão prejudicar ações –em curso ou a realizar num futuro próximo– na área da Política Externa de Segurança e Defesa (PESC/*Common Foreign and Security Policy–CFSP*) que necessitem duma componente funcional no Ciberespaço.

A emancipação da Cibersegurança da *eSociety* na União Europeia

Assim, depois dos atos terroristas de Madrid (2004) e Londres (2005), como corolários de Nova Iorque e Washington (2001), a preocupação com as ICs passou, de igual modo, para o topo das agendas da UE, ainda, ao abrigo da *eSociety i2010 initiative*. Deveremos referir a existência de vários documentos de interesse, que demostravam uma continuada preocupação com o "mega terrorismo" internacional, como foi o caso da '***Communication Critical Infrastructure protection in the fight against terrorism'*** publicada pela CE, em outubro de 2004, onde aquela «apelava aos EMs para aprimoraram as suas políticas relativas às PICs, para melhor se prepararem no sentido de um aumento da ameaça de ocorrência de ataques terroristas» (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 32). No dois anos subsequentes, foram publicados: 1. O '***Green Paper on a European Programme for Critical Infrastructure Protection'*** indexado por COM(2005) 576 final[LGR09], de 17 de novembro de 2005; 2. Foi melhorado no ano seguinte (2006) na '***Communication on a European Programme for Critical Infrastructure Protection'–EPPIC***. Nessa última comunicação, a CE registava «que as infraestruturas críticas na Europa estavam/[estão] intricadamente ligadas e altamente interdependentes e reconhece como aquelas eram/[são cada vez mais] dependentes das tecnologias de informação, incluindo a Internet e o espaço destinado às

identify the source of the attack. As a result, the boundaries between justice and home affairs policy on the one hand and foreign policy on the other become increasingly blurred. Threats can no longer be clearly defined as belonging to the area of responsibility of either policy field. A visible sign of this development in the increasing level of cooperation between authorities and institutions responsible for different policy fields. This erosion of traditional roles is more problematic in the EU than it is in the national context, but it is no means a new phenomenon. In the last years, the development of European security policy has largely been driven by an internationalization of the EU's justice and home affairs policy, […] In this new political structure, both the European Commission and the European Parliament gain new possibilities for influencing the policy-making process." (BENDIEK, "European Cyber Security Policy", 2012, p. 6)

comunicações de rádio navegação[58]». Esta abordagem, «de visão abrangente e a 'longo prazo', apela[va] a uma resposta Europeia às vulnerabilidades que pudessem advir dum resultado na falha de serviços essenciais»[59]. A ***EPPIC*** preconizava, como complemento, a criação duma rede de alerta que viria a ser a '***Critical Infrastructure Warning Information Network'*** – ***CIWIN***, estabelecida (conjuntamente com o respetivo portal https://ciwin.europa.eu/Pages/Home.aspx) em meados de janeiro de 2013[60]; 3. Ainda, quanto à identificação ou catalogação das PICs na Europa e respetiva avaliação na necessidade de melhorar a sua proteção, em 2008, foi publicada uma diretiva sobre PICs, indexada por 2008/114/EC[LRG22] –considerada, texto relevante para efeitos de (*Electric and Electronic Equipement–EEE*). Esta diretiva centrava-se nos «setores da energia e dos transportes, dando também, fundações bastante sólidas para ser estendida a outros setores, nomeadamente, ao das TICs, [vindo a sê-lo em 2011/2012]. A diretiva mencionava linhas de atuação gerais na gestão de riscos –designadas através de 'planos de segurança do operador'– e a necessidade de haver oficiais de ligação e relatórios obrigatórios, assim como, a partilha de informação, sensível, com as autoridades judiciais.» (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 33)

---

[58] "Global commons are domains that are not controlled by any single state; rather, they are universally needed and thus should be shared. These areas, or functions, of cooperation deemed to be central to life have traditionally included the high seas, airspace, and outer space. However, new issue areas, for example cyberspace, have recently been added to the list of global commons.* *Many include the polar areas and the electromagnetic spectrum in this listing. " (AALTOLA, SIPILÄ, & VUORISALO, 2011, p. 9)

[59] "Those physical resources, services, and information technologies facilities, networks and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Europeans or the effective functioning of the EU or its Member States governments." (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 32)

[60] "The set-up of the Critical Infrastructure Warning Information Network (CIWIN) is one of the measures foreseen to facilitate the implementation of the European Programme for Critical Infrastructure Protection (EPCIP). In October 2008, the European Commission issued a Proposal for a Council decision on a Critical Infrastructure Warning Information Network (CIWIN). The proposal aimed at assisting Member States and the European Commission to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of Critical Infrastructure Protection (CIP). The CIWIN network has been developed as a Commission owned protected public internet based information and communication system, offering recognised members of the EU's CIP community the opportunity to exchange and discuss CIP-related information, studies and/or good practices across all EU Member States and in all relevant sectors of economic activity. The CIWIN portal, following its prototype and pilot phases, has been up and running since mid-January 2013. DG HOME coordinates all activities relating to CIWIN and nominates the content manager of CIWIN. DG HOME consults the representatives of Member States – the CIP Points of Contact – on strategic issues in correlation with CIWIN. The CIP Point of Contact of the Member State nominates a CIWIN Executive and Support Officer who provide to the European Commission assistance in the context of the use and development of the CIWIN system. Information on the membership conditions as well as the registration and contact form may be found on the CIWIN portal." Retirado de http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm em 03/mai./2013.

Seguiram-se os restantes três documentos fundamentais, sendo um deles, uma diretiva destinada ao "todo-poderoso" setor das telecomunicações: O primeiro foi a '***Telecommunications Framework Directive***' –2009/140/EC[LRG23b], tendo passado a vigorar a 19 de dezembro de 2009 e que deveria ter sido adaptada aos quadros legislativos dos EMs até 25 de maio de 2011 –tendo sido publicada no JO L 337 de 18 de dezembro de 2009. Aquela, «Introduzia melhoramentos na diretiva anterior – 2002/21/EC[LRG02a] do PE e do Conselho de 07 de março de 2002 em relação ao regulamento de enquadramento das redes de serviços em comunicações eletrónicas ou, '*Framework Directive*'– no sentido de harmonização na legislação, com o enfoque especial na segurança». A diretiva representava «um passo decisivo no sentido de ser atingido um quadro-regulador destinado à ampla-comunidade da UE [cerca de 500 milhões de consumidores em 28 realidades], que deverá ser/ [deveria ter sido] transposta para a legislação de todos os EMs». Para isso, a *ENISA* foi chamada a colaborar de forma significativa «assumindo as responsabilidades associadas ao Artigo 13A[61] da revista '***Telecommunication Framework Directive'***. […] Sendo de esperar que a *ENISA* venha a desempenhar/[estando, já a desempenhar[62]] um papel relevante em

[61] "Chapter III (Security and Integrity of networks), Article 13A – Security and Integrity - 1. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services. Having regard to the state of the art, these measures shall ensure a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks. 2. Member States shall ensure that undertakings providing public communications networks take all appropriate steps to guarantee the integrity of their networks, and thus ensure the continuity of supply of services provided over those networks. 3. Member States shall ensure that undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services. Where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and the European Network and Information Security Agency (ENISA). The national regulatory authority concerned may inform the public or require the undertakings to do so, where it determines that disclosure of the breach is in the public interest. Once a year, the national regulatory authority concerned shall submit a summary report to the Commission and ENISA on the notifications received and the action taken in accordance with this paragraph. 4. The Commission, taking the utmost account of the opinion of ENISA, may adopt appropriate technical implementing measures with a view to harmonising the measures referred to in paragraphs 1, 2, and 3, including measures defining the circumstances, format and procedures applicable to notification requirements. These technical implementing measures shall be based on European and international standards to the greatest extent possible, and shall not prevent Member States from adopting additional requirements in order to pursue the objectives set out in paragraphs 1 and 2. These implementing measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 22(3)."

[62] "Q: How do you react to the fact that some businesses wish a complaint that may be can burn on them, regarding the breach notifications? A: I would say that, the Industry always crying. If you look at it the question is always a well safer regulation work. You have some examples of thus work, but on the other

relação à importância de aspetos de segurança no setor das telecomunicações na UE.» (KLIMBURG & TIIRMMA-KLAAR, 2011, pp. 33-34); No segundo –dos três– , ainda nesse mesmo ano de 2009, a CE através do '*Information Society and Media Directorate*'–*DG INFSO* (atual '***Co**mmunication **Ne**tworks, **C**ontent and **T**echnology'–DG CONNECT*[63] [64]), emanou uma comunicação intitulada '***Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience'*** e indexada por COM(2009) 149 final[LRG23] de 30 de março de 2009. Nela, a CE adotou a '*Communication on Critical Information Infrastructure Protection'* focalizada na proteção para a Europa das possíveis ciber-falhas contra as PICIs. O

---

hand was a responsibility of a national government and the European Commission and ENISA to give advice here, to say where something you need to support citizens of the small and medium companies. If you take an example, you can take «cloud computing». You as a citizen, you cannot negotiate SLS [*Service Level Specifications*] with a big provider. This is something a question were always we have to stimulate the market, do you have to support or to be behind citizens to have a equal situation in this business and in those cases the safer regulation those not work, the government does to do this." Doutor Udo HELMBRECHT, Executive Director of ENISA**,** to discuss ENISA's activities in the field of cyber security**.** Consultado em http://www.vieuws.eu/citizens-consumers/cyber-security-udo-helmbrecht-enisa/ a 10/mar./2014.

[63] "As of July 1 [of 2012], the DG Information Society and Media Directorate (DG INFSO) will change the name to Directorate General for Communications Networks, Content and Technology (DG CONNECT). "*Our new name better represents the range of topics where we are active, and our new structure better aligns the work of the DG with key EU policies for the coming decade: ensuring that digital technologies can help deliver the growth which the EU needs.*" (Robert Madelin, *Directorate General for the Information Society)*" em http://wbc-inco.net/object/news/10097; consultado a 06/mai./14. "The Commission yesterday, 25/04[/2012], announced that they will change to face the future: and launch "DG CONNECT". The Commissioner for the Digital Agenda for Europe, Neelie Kroes. The objective is *'to adapt and face the challenges of the next ten years*". They will change the structure, culture and mission of the DG (directorate general), and become '*more flexible, with fewer managers, less fragmented, and better finding the links between policy and research areas*.' They will also get a new name: "DG Connect", which stands for the key areas, they cover (Communication Networks, Content and Technology). 'DG Connect' also shows how the digital revolution is connecting and linking up Europe. The changes will take effect as of 1st July [/2012]." http://www.enisa.europa.eu/media/news-items/the-commission-changes-from-dinfso-to-201cdg-connect201d; Consultado a 06/mai./2012.

[64] "The Head of the DG INFSO, go on it will be DG CONNECT, is Robert MADELIN on Cloud Computing and the 'new' DG CONNECT. Q: Let it is start about the issue. It is changing it is name. What is that about and will DG CONECT be significantly different? A: So firstly, what is in the name, CONNECT, we want to connect with everybody else and we want people to connect with us and we think our business is connecting. So, connections in the more traditional communications network Internet sense, but also, connections between search communities and societies. So, for example, we want to invent it world class robots, that is Europeans thinks is a good idea. So, connections in a word sense and that is the word we want it to use. What is in the underlying change meant austerity? So will be a liner in Directorate General in the past, a few scenes of managers. Secondly multi disciplaniarity. So, in an area like cybersecurity, we will go be doing the Policy, the research and the regulation – all in one place – Not scatted around; Thirdly, delivery. So, instead say we want a competition in one part of our brain and investment on some else, we put it together in a single direction. So we want it connect internally also as well in the rest of the world. Q: Okay, now it comes in effect on July the 1st [2012]? A: Yes!" Consultado em www.vieuws.com/robert-madlin-on-cloud-computing-the-new-dg-connect/ em 08/06/2014. (In light of the 2nd Digital Agenda Assembly (21 + 22 June) leading technology journalist Jennifer BAKER met with Robert MADELIN, Director General of DG INFSO, to discuss Cloud Computing and the **'**new' DG CONNECT)

objetivo era melhorar a segurança e a referida **Resiliência**[65], e como consequência do «Plano de Ação acordado na Conferência Ministerial de Tallinn sobre a Proteção das PICIs», baseado em cinco pilares: (i) Preparação e prevenção; (ii) Deteção e resposta; (iii) Mitigação e recuperação; (iv) Cooperação Internacional; e, (v) Critérios para as ICs Europeias no campo das TICs; No terceiro documento –"Plano de Ação"– eram «anunciadas um número significativo de iniciativas, incluindo: o '*European Public Private Partnership for Resilience'–**EP3R***[66]; a criação de uma plataforma de alerta e partilha de informação, a '*European Information Sharing and Alert System'–**EISAS***[67]; a organização de exercícios de Cibersegurança ao nível europeu [*Cyber Europe 201x, x=10, 12, 14, ...*]; e a implementação de Equipas de Resposta Rápidas [*Computer Emergence Response Team–CERT*[68]*ou "aka", Computer Security Incident Response Team – CSIRT*, em "linguagem" da comunidade de Cybersegurança] plenamente

[65] "Resilience is the ability of a system or society to absorb and recover quickly after experiencing a sudden shock or physical stress." (BRUNNER & GIROUX, 2009, p. 1)

[66] "ENISA is currently involved in a key initiative to build closer partnerships between the public and the private sectors. An initial survey of critical information infrastructure protection (CIIP) in Europe revealed that the critical information infrastructures (CII) sector was fragmented both geographically and due to the competition among telecom operators. Increasing the Resilience of those CIIs was generally seen as fundamental within Member States and several National Public-Private Partnerships (PPPs) were already established to enhance preparedness and response to disasters or failures by coordinating the efforts among telecom operators. Cross-border mechanisms were set up on an *ad hoc* basis and soon a need for global approach at a European level arose to respond to both existing and emerging threats. In March 2009, the European Commission adopted a policy initiative - COM (2009)149[LRG23] - on Critical Information Infrastructure Protection (CIIP) to address this challenge and a European Public-Private Partnership for Resilience (EP3R) was established in order to support such coordination. The objectives of EP3R are fourfold: - Encourage information sharing and stock-taking of good policy and industrial practices to foster common understanding; - Discuss public policy priorities, objectives and measures; - Baseline requirements for the security and resilience in Europe; - Identify and promote the adoption of good baseline practices for security and resilience. EP3R will build upon national PPPs and engage both the public and private sectors in addressing the pan-European dimension of the resilience of critical EU-wide infrastructure. The European Commission requested ENISA to support the EP3R process and facilitate the establishment of three Working Groups which ENISA will support in several key areas." Em http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r consultado a 06/mai./2014.

[67] "EISAS stands for European Information Sharing and Alert System. ENISA has been asked by the European Commission to deliver a feasibility study on a Europe-wide sharing system for NIS related information to end-users/citizens and SMEs, to raise IT security awareness and close gaps in the coverage with such information." Em https://www.enisa.europa.eu/media/faq-on-enisa/faq-on-enisa-and-eisas. Consultado a 06/mai./2014.

[68] "Computer Emergency Response Teams (CERTs, aka CSIRTs) are the key tool for Critical Information Infrastructure Protection (CIIP). Every single country that is connected to the internet must have capabilities at hand to effectively and efficient respond to information security incidents. But CERTs must do much more. They must act as primary security service providers for government and citizens. At the same time, they must act as awareness raisers and educators. Not every country connected to the internet disposes of CERT capabilities. And the level of maturity among those who do vary dramatically. It is ENISA's mission to, as much as we can, clear out the "white spots" on the CERT world map and to minimise the gaps by facilitating setting-up, training and exercising of CERTs." http://www.enisa.europa.eu/activities/cert , consultado a 06/mai./2014.

funcionais até ao final de 2011 [p.e., o do Reino Unido, só recentemente foi considerado operacional][69], quer ao nível das instituições da UE, quer dos EMs.» Ainda dentro do plano do conceito de **Resiliência**[65] [70], o atual *DG CONNECT* «comprometeu-se a conceber um relatório designado por '***Principles and Guidelines for Internet Resiliense and Stability'***[71] que passou a ser um instrumento de trabalho central ao nível do Grupo de Trabalho UE-EUA sobre a Cibersegurança e o Cibercrime[72].» (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 33)

Estes princípios e linhas orientadoras para a estabilidade e resiliência na UE poderão contribuir para implementações de projetos de Investigação e Desenvolvimento

[69] "The British government has finally launched its Computer Emergency Response Team (CERT-UK), with the aim of bolstering the UK's defences against cyber threats ranging from hackers to state-sponsored attacks. First announced in December 2012 as a key element of government's £650m cyber security strategy, CERT-UK was initially supposed to launch by the end of 2013, but was delayed until 2014." Consultado em http://www.telegraph.co.uk/technology/internet-security/10734484/Government-launches-cyber-emergency-response-team.html, a 30/mai./2014.

[70] "The academic literature makes a distinction between two extremes: On the one hand, there may be a relatively swift recovery in which the system is restored to the next functionality that it was at before the incident ('bounce back'); on the other hand, there may be a dynamic, adaptative, and often longer-lasting process in which the system adapts to the new situation upon restoration of its functionality through processes of learning and adjustment ('adaptation'). (CAVELTY & PRIOR, 2012, p. 2)

[71] "On 30 March 2009, the Commission announced, via Communication COM(2009) 149 [LRG23], the launch of an action plan on Critical Information Infrastructure Protection. The main goal of the action plan – running from 2009 until 2011 – is to focus on a number of urgent activities which, according to the Commission, are necessary in order to strengthen the security and resilience of vital ICT infrastructures. The action plan was broadly supported by the Council of the European Union in December 2009. The CIIP action plan is part of a more extensive strategy of the European Commission to strengthen network and information security in the information society. It follows and complements Communication COM(2006) 251[LRG11] on a Strategy for a Secure Information Society, the legislative and non-legislative initiatives to fight cyber-crime and ensure online safety, and feeds into the "trust and security" objectives of the Digital Agenda or Europe, one of the flagship initiatives of the Europe 2020 strategy of the European Commission (COM(2010) 2020)[LRG25a]. […]"Lê-se no preâmbulo de março 2011, em http://ec.europa.eu/danmark/alle/110401_rapport_cyberangreb_en.pdf ; consultado a 06/05/2014.

[72] "An EU-US Working Group on Cybersecurity and Cyber Crime (EU-US WG) was established in the context of the EU-US summit of 20 November 2010 held in Lisbon. The Cyber Atlantic exercise is a result of the EU-US cooperation within this WG. The purpose of the EU-US WG is to address a number of specific priority areas and report progress on these within a year. The EU-US WG is composed of the following subgroups: Cyber Incident Management, Public-Private Partnerships, Awareness Raising, and Cybercrime. The Concept paper for the EU-US WG defines the scope of the activity and expected deliverables for the US-EU Summit later in 2011. In the area of Cyber Incident Management (CIM), the WG agreed to deliver a cooperation programme providing for synchronized and coordinated cyber exercises in the EU and US, culminating in a joint cyber exercise in 2013. In order to determine in which areas the EU and the US could cooperate regarding CIM, it was decided to organise a table top exercise, CYBER ATLANTIC, in November 2011. Future orientations of CIM will be based upon the results of CYBER ATLANTIC 2011, in order to build towards the joint cyber exercise in the near future." Em http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-atlantic;.
Para situação atual a 26/03/2014 http://www.eeas.europa.eu/statements/docs/2014/140326_01_en.pdf ; consultados em 06/05/2014.

(I&D/*Research and Development–R&D*) enquadrados no Programa *Horizon* da estratégia da UE 2020, cujo gestor será o Comissário indigitado (e tacitamente aceite pelo PE), por Portugal, Senhor Engenheiro Carlos Manuel Félix MOEDAS, que terá um orçamento aproximado de 80 mil milhões de Euros até 2020 para o efeito.

A "parente-pobre": A Política Externa de Segurança Comum da União Europeia

Tomando em conta, «as preocupações com as políticas RSI enquadradas na PESC[73], e comparadas às mesmas políticas RSI relativas ao conjunto PICIs e Cibercrime[74], as primeiras, estão muito menos desenvolvidas». Em parte, «devido à sua natureza confidencial e interdepartamental, mas também, devido a causas que se prendem com as dificuldades inerentes à abordagem a estes assuntos junto dos EMs,» (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 29) por parte das instituições da União – CE, Conselho e PE. Isto, porque podem ser percetíveis *a priori* como matérias à consignação preferencial dos EMs da União, em particular, «[…] o papel na PESC no plano da política de Cibersegurança encontra-se confinado às ações dos cinco EMs dominantes (Alemanha, França, Reino Unido, Holanda e Suécia). […]» (BENDIEK, "European Cyber Security Policy", 2012, p. 6) [ver Seção **1.3 e** Seção **1.4 do Capítulo 1, Políticas de Segurança do Ciberespaço na UE]**

Esta problemática –das políticas RSI relativas à PESC– está subjacente e necessariamente, relacionada com a Estratégia Europeia de Segurança (EES/*European Security Strategy–ESS*[75]). Começou a ser abordada – ainda no mandato do senhor

[73] "Cyber-initiatives within the European Common Foreign and Security Policy (CFSP) area have been far less developed compared to CIP or crime areas." (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 34)

[74] "Broadly speaking, cybercrimes is defined as combination of 'criminal acts transformed by networked technologies' (WALL, 2006/7) [*]. Even if there are several categorizations of cybercrime offences[**], this work distinguishes: - Offences against the confidentiality, integrity and availability of computer data and systems; - Computer-related offences; - Computer content-related offences. This categorization is based on the CoE Convention[***] and UNODOC[****] 'Comprehensive Study on Cybercrime'. [*]WALL, D., '*Policing Cybercrime'*, in Criminal Justice Review, University of Leeds, 2006/7. [**]For other categorizations see FAFINSKI, S. et al. (2010) and WALL (2006/2007). [***]Despite that the Article 1 of the CoE Convention has the title 'Definitions' it does not contain any specific definition of the word cybercrime. However, the Chapter II of the Convention recognizes cybercrime under four titles. [****]United Nations Office on Drugs and Crime " (NOTO, 2013, p. 3)

[75] "Cybersecurity was identified as a key security issue in the report on the implementation of the European Security Strategy (ESS) submitted by SG/HR Javier Solana to the European Council in December 2008. In a subsequent 2009 workshop at the EUISS [European Union Institute for Security Studies], a seminar was held to initiate a first discussion on the implications of the cybersecurity agenda for the EU as a whole and examine ramifications of cyber for the CFSP. The event was organized jointly with the General Secretariat of the Council of the EU and in cooperation with Estonia[*] [*]See Institute for Security Studies, Cybersecurity: what role for CFSP?, 4 February 2009, http://www.iss.europa.eu/nc/seminar/select_category/26/article/cyber-security-what-role-for-cfspbrbrussels-4-february-2009/?tx_ttnews[pS]=1230764400&tx_ttnews[pL]=31535999&tx_ttnews[arc]=1&cHash=206ccab0a (não encontrado a 07/mai./2014, porque provavelmente temporariamente desativado)" Encontrado em

Secretário Geral/Alto Representante, Javier SOLANA, como responsável pela PESC, aquando da «implementação do relatório sobre a Estratégia Europeia de Segurança, adotado em 2008. Já incluía as ciber-ameaças como uma nova categoria, quanto ao risco e sua complexa e difícil gestão[76] para a Segurança Europeia». O relatório, de 11 de dezembro, indexado por S407/08[LRG108a], refere, especificamente, quanto à Cibersegurança nas páginas 1 e 5:

> "Globalisation has brought new opportunities. […] But globalisation has also made threats more complex and interconnected. The arteries of our society – such as information systems and energy supplies – are more vulnerable. " p.1
>
> Modern economies are heavily reliant on critical infrastructure including transport, communication and power supplies, but also the internet. The EU Strategy for a Secure Information Society, adopted in 2006 addresses internet-based crime. However, attacks against private or government IT systems in EU Member States have given this a new dimension, as a potential new economic, political and military weapon." p.5 Consultar em http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf; Acedido a 30/mai./2014.

Recomendava ainda, «que fosse desenvolvido trabalho adicional nessa área, explorando uma abordagem compreensiva por parte da UE (ver diagrama na p. 28), dando relevo à importância do assunto e alertando para a necessidade no incremento da cooperação internacional.» (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 34) No ano

---

www.iss.europa.eu/uploads/media/Report_cyber_security_1_.pdf a partir de http://www.iss.europa.eu/activities/detail/article/cyber-security-what-role-for-cfsp/ a 19/jun./2014.

[76] "[…] While risk assessment methodologies have a long tradition in cyber-security, they are also fundamentally flawed in the context of complex networks and complex risks, because they build on linear methods, whereby an extrapolation into the future is done on the basis of past experience. As long as cyber-security issues have been on the political agenda, the debate has been characterized by the struggle of various practitioners and security specialists to determine how big the threat really is (Dunn CAVELTY 2008)[*]. The main reason for this is there is an incomplete view of the frequency and gravity of cyber-incidents in individual companies and the government networks, i.e. because these actors do not have sufficient incident detection capabilities or because they are not forthcoming with the information. Therefore, there is even far less knowledge about the exposure in whole business sectors let alone on an aggregated level of countries, much less on the level of the EU. Attempts to collect and aggregate data beyond individual networks have failed due to insurmountable difficulties in establishing what to measure and how to measure it and what to do about incidents that are discovered very late, or not at all (SOMMER and BROWN 2011:12; SUTER 2008; ROBINSON et al. 2013: 58)[**] […]. [*]CAVELTY, Myriam Dunn (2008) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, London: Routledge [**]Sommer, Peter & Ian Brown (2011) Reducing Systemic Cyber Security Risk, Report of the International Futures Project, IFP/WKP/FGS(2011)3, Paris: OECD. – SUTER, Manuel (2008) 'Improving Information Security in Companies: How to Meet the Need for Threat Information': in Dunn CAVELTY, M., MAURER, V. & KRISHNA-HENSEL, S.F. (eds), *Power and Security in the Information Age: Investigation the Role of the State in Cyberspace*. Aldershot: Ashgate. – ROBINSON, N., HORVATH, V., CAVE, J. ROOSENDAAL, A. (2013) Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts, Committee on Industry, Research, and Energy. " (CAVELTY M. D., "A Resilient Europe for an Open, Safe and Secure Cyberspace", 2013, p. 5)

seguinte, a 4 de fevereiro de 2009, realizou-se um seminário organizado pelo Instituto de Segurança Europeu, em Bruxelas, intitulado '*Cyber Security: what role for CFSP?'* que gerou um relatório embrionário –não conclusivo, porque originado em *brainstorming*– indexado por IESUE/SEM(09)04[LRG109] [77], de 10 de março de 2009. Consultado em (www.iss.europa.eu/uploads/media/Report_cyber_security_1_.pdf a partir de http://www.iss.europa.eu/activities/detail/article/cyber-security-what-role-for-cfsp/ a 19 de junho de 2014.)

As questões sobre a ESE[78], assim como, a Estratégia de Cibersegurança da UE (ECS/*Cyber Sscurity Strategy–CSS*)[79] (ver Seção **1.6**, **A UE: Um Ciberespaço Aberto, Seguro e Protegido**) e relativas à Estratégia de Segurança Interna da UE (ESI-*Internal*

[77] "[…] The seminar's goal was to initiate a first discussion (brainstorming) on the implications for the EU of the cyber security agenda and related threats: to raise subject awareness, and to identify a number of critical issues for the possible development of a policy under the Common Foreign and Security Policy (CFSP) that would be part of a comprehensive approach by the EU in this area." (ZANDERS, Jean-Pascal, 2009, p.1)

[78] "Yes, Europe's leadership has to focus on resolving the economic and financial crisis. But the more limited the means, the more crucial it is to prioritize and make sure that the means the policy-maker does have are put to use in the most relevant way. 'Gentlemen, we have run out of money. It's time to start thinking', to quote Sir Winston CHURCHILL (who else)[*] Does the existing European Security Strategy (ESS), adopted in 2003, do all of this? No. The ESS tells us how to do things, but not what to do. It mostly concerns the instruments: the ESS codifies the (important!) choice for a preventive, holistic or comprehensive, and multilateral way of doing foreign policy. But to achieve which specific priority objectives? The ESS itself does not provide those, nor has it been used as a basis to develop them. So the argument to review the ESS is not that it is not viable. Quite the contrary: the choice for a preventive, holistic and multilateral foreign policy is the right one. But the choice of instruments should not be confused with the choice of objectives: doing things the right way is insufficient if one doesn't know why one does them. The reason why the EU needs more strategy is that the ESS is incomplete. The ESS definitely is a milestone in European strategic thinking, but it should not be its terminus." (BISCOP, 2012, p. 2) [*]Frase presumivelmente atribuída a Sir Winston CHURCHILL mas também podendo ser do físico Neozelandês, Sir Ernest RUTHERFORD.

[79] "I: Today we are talking about Cyber Security. Joining me to looking in the details of that is the Dutch MEP, Sophie in´t VELD. Q: Let's talk about Cyber Security. *[...]*, the announcement has been delayed and so forth, but you think quite vocal your criticism of the draft has been circulating? A: I am critical because that does not seem to be a very good definition of what Cyber Security really is. It seems to range from a, you know, secure payment systems, for paying on the Internet or the way down to the National Security and everything in the between, and I think, you know, the instruments they want to use for cyber security also are very wide ranging and I think we should distinguishes very clearly between law enforcement on one hand, and let's say, security and defence instruments on the other, and that of course you choose to have to do more with the Single Market or law enforcement at all, and it mixing that all up, and I think in a democracy that is wrong. In a democracy, law enforcements not security, is not a Single Market; Q: Well the Single Market was a big issue, that, we want free flow information and certainly want a more harmonized approach because the Internet does not respect boarders, so why they to put it all in a document that is all about defence all the boarders, if you like, of Europe? A: If, you know, we need, you say Cyber Security that sounds very interesting and everybody will agree readily that Cyber Security and security systems, but if you look more closely, you can see that this strategy is not a strategy, it's just a mishmash of different measures and I think we are on a slippery slope. Because if you look at, for example, illegally downloading or hacking, you know, certainly illegally downloading isn't a matter of National Security, cam 'on! […]". Consultado em http://www.vieuws.eu/ict/eu-cyber-security-mep-in-t-veld-laments-lack-clear-strategy/ a 08/out./2013.

Security Strategy–ISS)[80] continuam na "ordem do dia" das agendas Europeia, e não são pacíficas: Quer quanto à sua génese e natureza e/ou validade, quer quanto aos procedimentos decorrentes das mesmas e suas possíveis concretizações; Não há certezas, quanto às consequentes implicações políticas das suas não redefinições "à luz" de novos desenvolvimentos da política global, às sobreposições de soberanias entre as instituições da União, nomeadamente o PE, a CE, o Conselho e os EMs[81]. Assim como, os verdadeiros interesses, de alguns dos últimos (em particular de cinco deles, atrás referidos, p. 4 e p. 20), e os daquelas instituições, face aos resultados das últimas eleições de maio passado (aumento de Membros do Parlamento Europeu MPE/*Member of European Parliament–MEP,* de "forças" políticas eurocéticas).

Ainda quanto às implementações específicas, no domínio da Cibersegurança, aliadas a ações no plano da PESC**,** «a Agência Europeia de Defesa (AED/*European Defence Agency–EDA*) e o Conselho Militar da UE/*EU Militar Committee–EUMC*, têm desenvolvido trabalhos na área»[82]. Nomeadamente, «desde 2008, nos aspetos relativos às chamadas Operações sobre Redes de Computadores ou *Computer Network Operations–CNO*[83]*»* (ver diagrama da p. 25). As interceções entre *CND*, *CNE* e *CNA* não estão perfeitamente definidas e continuam a ser «alvo de polêmica e acesa

[80] "The adoption of an Internal Security Strategy (ISS) for the European Union (EU) caught many Brussels watchers off-guard. Appearing rather quickly from the hands of the Spanish Presidency in 2010, the ISS was adopted without widespread debate in the early months of that year. Since then, commentators have taken aim at the ISS, what it means for the EU, and what it may (or may not) represent for the future of internal security policymaking in the EU. Most analysts, however, fail to take into account the historical, institutional and political context from which the ISS emerged. This paper shows that the ISS has a much longer lineage than typically assumed, and argues that the background of the ISS must be accounted for if we are to gauge its potential to shape the future direction of EU internal security cooperation." (HORGBY & RHINARD, 2013, p. 4)

[81] "An EU grand strategy should prioritize those foreign policy issues that[*] are the most important for all Member States because they most directly concern the vital interests that they all share and[**] on which there is the greatest added value in collective action by the Union and the Member States. The result should be a short list of priorities, not for all eternity, as a declaration of principle, but for the next five years, as a mandate for all of the EU institutions – as an agenda for comprehensive action, now. [*]Colin S. GRAY, *The Strategy Bridge. Theory for Practice* (Oxford: Oxford University Press, 2010), p. 28. [**]Sven BISCOP & Jo COELMONT, *Europe, Strategy and Armed Forces. The Making of a Distinctive Power* (Abingdon: Routledge, 2012)." (BISCOP, 2012, p. 4)

[82] "Around the same time [2008], the EU military authorities initiated the first steps to examine the feasibility of developing a common doctrine on **CNO** (i.e. cyberwar)." (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 34)

[83] "Within the concept of cyberwar, a distinction must be made between three forms of Computer Network Operations (CNO). The deliberate paralysation or destruction of enemy network capabilities is called a Computer Network attack (CNA). Such attacks may be complemented [or anticipated] by Computer Network Exploitation (CNE), which aims at retrieving intelligence-grade information from enemy computers by means of IT. Finally, Computer Network Defence (CND) includes measures to protect own computers and computer systems against hostile CAN and CNE." (CAVELTY M. D., "Cyberwar: Concepts, Status quo, and limitations", 2010, p. 2)

discussão ao nível da Academia, dos *think-tanks* internacionais relacionados com o campo da Estratégia, Geopolítica e Segurança e dos decisores político-militares[84]». Não é credível, em certos meios, sequer a assunção do termo Ciberguerra[85], mas sim como «uma terrível metáfora» (SCHMIDT, 2011, p. 49). Logo, um termo totalmente inadequado, porquanto «o potencial de utilização do Ciberespaço num conflito parece óbvio quanto às atuais e efetivas propriedades do Ciberespaço, tornam conceitos fundamentais de ***ataque***, ***defesa***, e mesmo de ***guerra*** inadequados;» Isto, pelo menos no plano estratégico[86]. Na mesma linha, outros autores sugerem, mesmo, a sua rejeição[87].

---

[84] "I have one topic that I want to touch on here, which is 'CNE and CNA', and that is maybe a kind of bureaucratic for some folks listening, but if you had been working for the government, the idea on that, is cyber espionage and cyber attack are two different things and they belong to perhaps two different organizations, and I think one of the things is that probably behind that and on sometimes is hard to tell the difference between in cyber offence and cyber defence. I think the largest the skills set, sometimes the hacker can just be someone who knows your network better than you do and uses that information for nefarious purpose. The virtual skills on some way and one of the philosophical and practical debate in Washington DC, is the difference between – Computer Network Espionage or Computer Network Exploitation (CNE) and Computer Network Attack (CNA). And what is the difference and I know what do you want to it if on defence you had to decide why a hacker is on your network and this is fascinating, because it either be could not an attacker perspective, to steal your intellectual property, they could also be the preparation for war in that an adversary would like to own your network (deeply on your network), so in a crises in the future they could be have the same level of coercion, some ability of influence, not only your organization does, that maybe in your nation, your leadership does. In terms of war or terrorism or international crime, who knows? […]!" Seminário Web da autoria de Kenneth GEERS, Senior Global Threat Analist da empresa FireEye Inc., com a duração de 59':17" relacionado com (GEERS, 2013) que pode ser ouvida, após simples registo, em https://www.brightalk.com/webcast/7451/88921 entre 43´:14" e 46´:02". Consultado a 01/06/2014. Complementar com o suporte da bibliografia em http://www.fireeye.com/blog/technical/threat-intelligence/2013/09/new-fireeye-report-world-war-c.html

[85] "In order to determine the substance and relevance of the concept of 'cyberwar', we require not only a lexical definition, but also a differentiation between the operative and strategic dimensions of cyberwar. We must distinguish between offensive and defensive cyberwar measures, with the role of the military in cyber defence being a limited one." (CAVELTY M. D., "Cyberwar: Concepts, Status quo, and limitations", 2010, p. 1)

[86] "Although cyberwar is not necessarily good for civilization, fears of its destabilizing effect are exaggerated. Besides being easily trumped by nuclear weapons and most forms of conventional conflict, the primary characteristics of cyberwar – its temporary effects, covert characteristics, the impossibility of disarming cyberwarriors, and the usefulness and primacy of cyberdefense – do not lend themselves to rapid uncontrollable action – reaction cycles. Cyberwar may take place at the speed of light, but this hardly suggests that strategic decisions about the use of cyberwar have to take place any faster than the speed of understanding." (LIBICKI, FALL/WINTER 2011, p. 78)

[87] "Thomas Rid's paper for The Journal of Strategic Studies has the provocative title 'Cyber War Will Not Take Place'[http://thomasrid.org/no-cyber-war/]. RID's argument is relatively straightforward. He uses CLAUSEWITZ to define the three characteristics of war: 'Any act of war has to have the potential to be lethal; it has to be instrumental; and it has to be political.' To be instrumental, according to RID, there has to be a means and an end. 'Physical violence or the threat of force is the means. The end is to force the enemy to accept the offender's will.' Then he uses published sources to list examples of cyber war (thankfully he avoids using the more common and in my opinion erroneous term 'cyberwar') and shows how none of those examples meet each of the three criteria. In brief, Professor RID concludes that there has never been an act of cyber war and that there probably will never be one (his final sentence leaves room for an 'act of Cassandra')." Consultado em http://jeffreycarr.blogspot.pt/2011/10/clausewitz-and-cyber-war.html . Consultado a 01/jun.2014. E http://www.forbes.com/sites/seanlawson/2011/10/26/cyber-war-and-the-expanding-definition-of-war/ Consultado, também a 01/jun./2014.

Isto, devido a não consistir «em elementos fundamentais formulados por CLAUSEWITZ» (TABANSKY, 2014, p. 8), levando à insinuação que se trata apenas de um "chavão", «*buzzword*» (CAVELTY M. D., "Cyberwar: Concepts, Status quo, and limitations", 2010), *sound-byte* ou definição abusiva e, totalmente, fora de contexto. O objetivo será potenciar a venda de livros, jornais e de veicular notícias genéricas para consumo generalizado e imediato, que provocam, invariavelmente, sensacionalismo e alarmismo na população em geral.

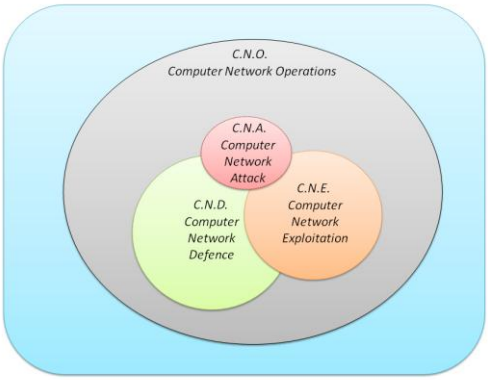

Ilustração 1- Diagrama de *Venn* –do autor baseado em (CAVELTY M. D., 2010) e (GEERS, 2013)– das *CNO*.

Legenda: *CNO*–Operações em Computadores em Rede; *CND*–Defesa de Computadores em Rede; *CNE*–Reconhecimento de Computadores em Rede (Recolha/ «Exfoliação» ou Espionagem): e, *CNA*–Ataque a Computadores em Rede (A CNA n presente só tem interesse operacional ou tático. No futuro, poderá ter interesse estratégico, se for possível implementar este tipo de ataque, unicamente ao nível virtual.)

Por outro lado, outros autores defendem, por exemplo, que o *worm*[DT&T02] [88](ver Anexo A.ii) ***Stuxnet***[89] foi o primeiro «míssil cibernético» da História e condicionará o futuro[90] da própria Ciberguerra[91]. Ele permitiu «uma exploração do Ciberespaço com

[88] Definições Técnicas e Tenologia relativas aos temas constantes deste trabalho. Para informações complementares, consultar o Anexo A.ii.

[89] "Stuxnet[DT&T01] (ver Anexo A.ii) was a proof of concept that cyber war can be real. And as the Department of Homeland Security recently noted, now that information about Stuxnet is publicly available, it's much easier for other bad actors to develop variants that target other SCADA[DT&T05] (ver Anexo A.ii) systems around the world. Because SCADA systems are pervasive and generic, the Stuxnet worm[DT&T02] (ver Anexo A.ii). is, essentially, a blueprint for a host of infrastructure attacks." (ROSENZWEIG, 2013, p. 6)

[90] "The most profound similarities between atomic weapons and cyber threats, however, lie in the disruptive nature of the Stuxnet[DT&T01] event (ver Anexo A.ii). Imagine what it must have been like the day after the first atomic bomb was exploded. Around the globe, settled assumptions about war, policy, foreign affairs, and law had, in an instant, all come unglued. Even 17 years after the atomic bomb was first exploded, the uncertainty about the use of these weapons and the threat they posed was so great that the Cuban missile crisis nearly engulfed the world in nuclear war. We are on the verge of experiencing the some sort of tumultuous time, and almost nobody in America – except a few senior policymakers – knows it. Perhaps more ominously, even at the dawn of the nuclear age, we were confident that we could identify anyone who used atomic weapons, and they would all be peer nation-state actors. In cyber realm,

sucesso, tendo como alvo –a camada de controlo de um processo industrial complexo, por forma– atingir uma meta destrutiva, tudo isto evitando uma confrontação militar.» (TABANSKY, 2014, pp. 7-9) Muitos autores têm analisado e trabalhado o tema da *cyber warefare* e o conceito *cyberwar*, assim como, as respetivas aplicações teóricas. Por exemplo, a académica Suíça, Myriam Dunn CAVELTY preconiza o plano tático-clássico da sua utilização, mas agora na «era da informação» como: «o termo '*cyberwar*', refere-se a uma subseção da utilização da informação na 'arte' de fazer ou conduzir a guerra no 'campo-de-batalha' [ou *warfare*]. Na parte deste amplo conceito, o qual pretende referir-se à influência no 'querer' e nas capacidades decisórias dos líderes políticos inimigos e das suas forças armadas e/ou nas atitudes das populações civis no teatro de operações ao nível das informações e dos sistemas de informação [*SIs* das *TICs*][*]. [*](cf *CSS Analysis* n.º 34 do mesmo Centro de Estudos de Segurança/*Center for Security Studies–CSS*, do Instituto Tecnológico de Zurique/*Eingenössische Technische Hochschule–ETH*)» (CAVELTY M. D., "Cyberwar: Concepts, Status quo, and limitations", 2010, p. 2) Acrescenta, ainda, que «a ciberguerra inclui atividades no Ciberespaço. Concetualmente, no entanto, a ciberguerra reflete o incremento da natureza tecnológica da guerra na era da informação, baseada na computação, eletrónica, e nas redes de comunicação e informação presentes em todas as áreas e aspetos de funcionamento de ações militares.»

Centrando-nos na UE e no tópico da possível utilização –direta– de *CNOs* (no apoio a ações humanitárias e de segurança no âmbito da PESC), estas deverão ser equacionadas com a necessária ponderação a nível tático/conjuntural e com extremo cuidado a nível estratégico, no futuro. Isto porque, as *CNOs*, intercetam a área adjacente da Ciberdefesa, logo, particularmente sensível a um número substancialmente significativo de EMs (nomeadamente, das suas Forças Armadas), aparentemente disjunta das prioridades políticas internas e algumas externas da UE.

---

we have much greater difficulty identifying who 'fires' the weapon, and th culprit may well be a non-state actor – perhaps a terrorist or a small group of hackers." (ROSENZWEIG, 2013, p. 7)

[91] "A cyber attack on Iran's nuclear programme may have forestalled more violent action, but such weapons cut both ways. 'Stuxnet´s Future of Cyber War' de FARWELL, James P. e ROHOZINKY, Rafal em Survival: Global Politics and Strategy February-March 2011 pp. 23-40, Vol 53, N.º 1, 01/fev./2011. Consultado em http://www.iiss.org/en/publications/survival/sections/2011-2760/survival--global-politics-and-strategy-february-march-2011-f7f0/53-1-05-farwell-and-rohozinski-f587 a 01/jun./2014.

No que a este trabalho diz respeito, (**excluindo, os respetivos procedimentos internos, confidenciais e inerentes a ações operacionais adstritas às instituições militares dos EMs e da OTAN, por razões óbvias de sensibilidade das informações e dificuldades de acesso às mesmas**) uma das hipóteses, dentro do âmbito da possível cooperação com a OTAN, seria justamente colmatar esta brecha de deficiência na articulação e operacionalização ao nível da UE, direcionada para a PESC. Evitar-se-ia a sobreposição de recursos financeiros, logísticos e humanos –escassos no presente. Aproveitava-se a realidade de simultaneidade de pertença da, quase, totalidade dos EMs a ambas as organizações. O último Conselho Europeu de dezembro passado, que abordou questões relacionadas com a PESC, a AED, a Cibersegurança entre outras [que teve por base o relatório elaborado e apresentado, a 15 de outubro de 2013, em Bruxelas, pela Vice-Presidente/Alta-Representante (VP/AR-*Vice-president/High Representative–VP/HR*) Senhora Catherine ASTHON[92]], deixa canais de exploração bem definidos nesta matéria, apesar de «a capacidade operacional de suporte a deliberações políticas do Conselho, e as ações da VP/AR e responsável pelo SEAE serem [ainda, em 2014] muito limitadas[93].» (Ver diagramas pp. 28-29)

> "However, given the current relatively weak wider institutional framework of common EU command and control capabilities, it will be hard for the EU to build common cyberdefence capabilities, even within the relatively limited areas of

[92] "As regards Cyber Defence, the objective is to establish a comprehensive and cooperative European approach. EDA activities, based on the recently adopted cyber strategy, focus on realistic deliverables within its remit and expertise: training and exercises, protection of headquarters, and Cyber Defence Research Agenda (focusing on dual use technologies)." Consultado em http://eeas.europa.eu/statements/docs/2013/131015_02_en.pdf , na p. 18, a 30/mar./2014.

[93] "There are also few appropriate structures for advising the Council and/or COREPER II[*] on cyber-issues or serious cyberattack. Serious cyberattack has until now been the domain of the Council Security Committee (INFOSEC) – a high-powered but secretive body that mostly concerns itself with Information Assurance issues[**]. Information Assurance is an absolutely critical area that directly impacts the existential security on the EU institutions; however INFOSEC does not have a CFSP mandate and therefore does not inform the CFSP – relevant bodies – even when there has been a probable state-sponsored cyberattack on EU institutions, something which has happened repeatedly in recent years at least. They do not directly inform COREPERII, which remains the responsibility of the Political and Security Committee (PSC/COPS).The PSC has support for military crisis management (EUMS) and civilian crisis management (CIVCOM), but not for cyber-issues. The recent established Committee on operational cooperation on internal security (COSI) might be able to fulfill this role. However, if so, the narrowly defined 'home affairs' mandate of this Committee may be as inappropriate for responding to serious cyberattacks as an excessively military or CFSP mandate would be. [*]COREPER II ('Committee of Permanent Representatives') is one of the most senior decision making bodies within the EU. It consists of heads of mission (Ambassador Extraordinary and Plenipotentiary) and deals largely with political, financial and foreign policy issues. – [**]Information Assurance is the practice of managing risks related to the use, processing, storage, and transmission of information or data and systems and processes used for dealing with sensitive information, whereby various levels of protection (such as encryption, or shielding of electronic radiation) is applied to various levels of confidentiality. The EU recognizes four security classification levels." (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 35)

'operational CNO' that have already been explored within the EU Battlegroup framework[i] Unless the EU militaries can establish a joint governance model for its communications and information system, progress in the area of cyberdefence will be very slow. And can at best achieve only a limited joint integrated capability. The **European Defence Agency** has carried about a few research projects on technology aspects related to cyberdefence, and is looking forward to cooperating with other international organizations is this field.[ii]" (KLIMBURG & TIIRMMA-KLAAR, 2011, pp. 34-35)[i] SIMÓN, Luís, 'Command and Control? Panning for EU military operations', *EUISS Occasional Paper*, n.º 81, January 2010, http://www.iss.europa.eu/uploads/media/Planning_for_EU_miltary_operations.pdf . [ii] See HALE, Julian, 'New EDA Chief Exec Looking to Show Agency's Added Value', *DefenceNews*, 11. January 2011 http://www.atlanticcouncil.org/blogs/natosource/new-eda-chief-exec-looking-to-show-agencys-added-value, consultado a 25/set./2014.

Estes canais exploratórios, como atrás referido, para um trabalho a médio-longo prazo, foram confirmados pelo Conselho a 19 e 20 de dezembro p.p., quando é dito na página quatro: «a definição, em 2014, de um Quadro de Política de Ciberdefesa da UE, com base numa proposta a apresentar pela VP/AR, em cooperação com a CE e a AED;» ou como está escrito na página seis: «Ciberquestões: elaboração de um roteiro e de projetos concretos centrados na formação e nos exercícios, melhoria da cooperação civil-militar [supostamente, também, na cooperação UE-OTAN (Ver Capítulo 2.)], com base na Estratégia da UE para a Cibersegurança [UE-ECS], bem como proteção dos meios nas missões e operações da UE.»

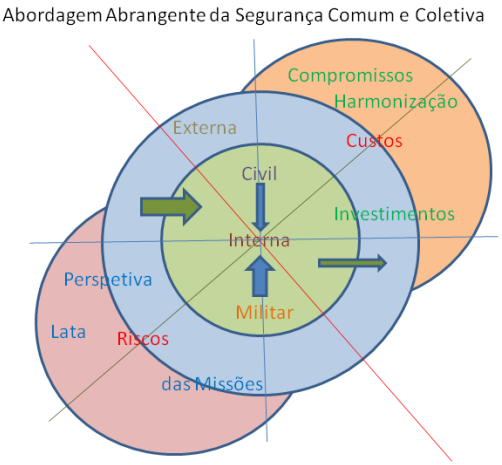

Ilustração 2- Diagrama –do autor baseado em (NUNES, 2012)– da visão abrangente da PCSD na UE

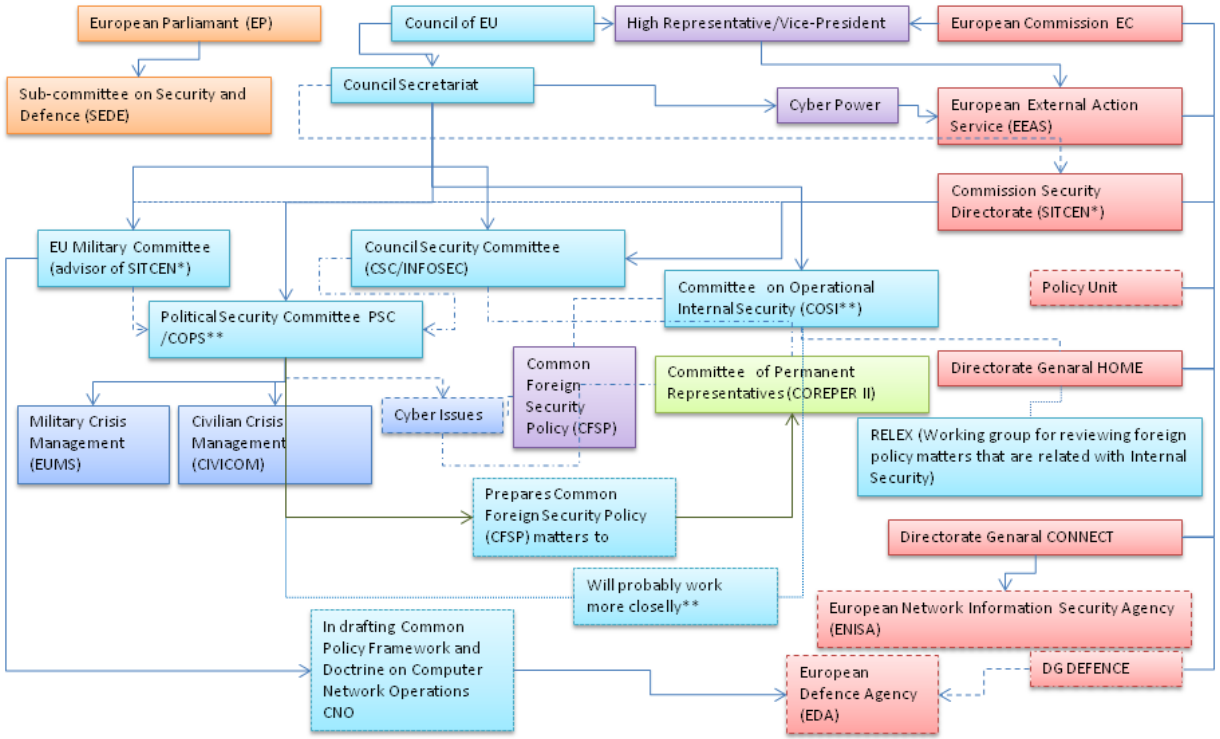

Ilustração 3- Diagrama –do autor, baseado em (KLIMBURG & TIIRMMA-KLAAR, 2011)– das funcionalidades da PESC e a Cibersegurança na UE

A Agenda Digital[94] e a Estratégia de Cibersegurança[95] da UE

Com a entrada em funções da CE-"Barrroso II" que cessa agora o seu mandato, foi incumbida a Comissária, então designada pelo Governo Holandês, senhora Nelie KROES e o, já referido, *DG CONNECT*, de implementar um desafio complexo e imenso que se designou por «Agenda Digital/*Digital Agenda*». Esta agenda –com as suas catorze Ações (ver quadro, pp. 31-32)– tem vindo a ser implementada, "passo-a-passo", ora com obstáculos e dificuldades –devido à complexidade dos assuntos e a, natural, resistência à mudança por parte dos atores, alguns "muito poderosos", no terreno–, ora com pequenos sucessos[96] No que a este trabalho concerne, interessa aprofundar o chamado Pilar III–Confiança e Segurança (ver a seção 1.2. do Capítulo 1) Para além deste último, a ***Digital Agenda*** é composta por mais seis Pilares, a saber: *I–Digital Single Market–DSM; II–Interoperability & Standards; III–**Trust & Security*** (o Pilar da Confiança e Segurança, acima referido)*; IV–Fast and ultra-fast Internet access; V–Research and Innovation; VI–Enhancing digital literacy, skills and inclusion; e, VII–ICT-enabled benefits for EU society*.

---

[94] "Digital Agenda for Europe, which includes 14 actions aimed at improving Europe's capability to prevent, detect and respond to network and information security problems." (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 32) COM (2010) 254 final/2, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:PT:PDF; [LRG27] de 26/ago./2010, Acedido em 08/mar./2014

[95] "Information systems can be affected by security incidents, such as human mistakes, natural events, technical failures or malicious attacks. These incidents are becoming bigger, more frequent, and more complex. In response, the European Commission releases its Cyber Security Strategy on Thursday 7 February."; "Most recently, the European Commission released its own Cybersecurity Strategy, entitled 'An Open, Safe and Secure Cyberspace'[LRG33], paired with a somewhat bold Directive ('The NIS Directive' [LRG34], that offers to tackle some of the core problems of cybersecurity governance (European Commission 2013a*, 2013b**) *European Commission (2013a) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) final; **European Commission (2013b) Proposal for a Directive of the European Parliament and the Council concerning measures to ensure a high common level of network and information security across the Union, 2013/0027(COD) http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/0027%28COD%29 consultado em 06/mai./14." (CAVELTY M. D., "A Resilient Europe for an Open, Safe and Secure Cyberspace", 2013, p. 4)

[96] Como foi o caso, recentemente anunciado, da abolição do *roaming* no Mercado Único Europeu (MUE/*European Internal ou Single Market – ESM)* a partir de 15 dezembro de 2015, conseguido em tempo *record*, inferior a um ano (segundo palavras da senhora Comissária KROES (01'33" a 01'39" da entrevista de 10 de outubro de 2013 em http://www.vieuws.eu/eu-institutions/commissioner-kroes-defends-eu-telecoms-package/ consultada a 31 de março de 1014], devido a ter sido introduzido numa proposta *package* da própria, destinada à poderosa indústria das telecomunicações e serviços de Internet, logo, houve outras contrapartidas para a perda de tal *cash cows* de uma matriz tipo *Boston Consulting Group – BCG*.

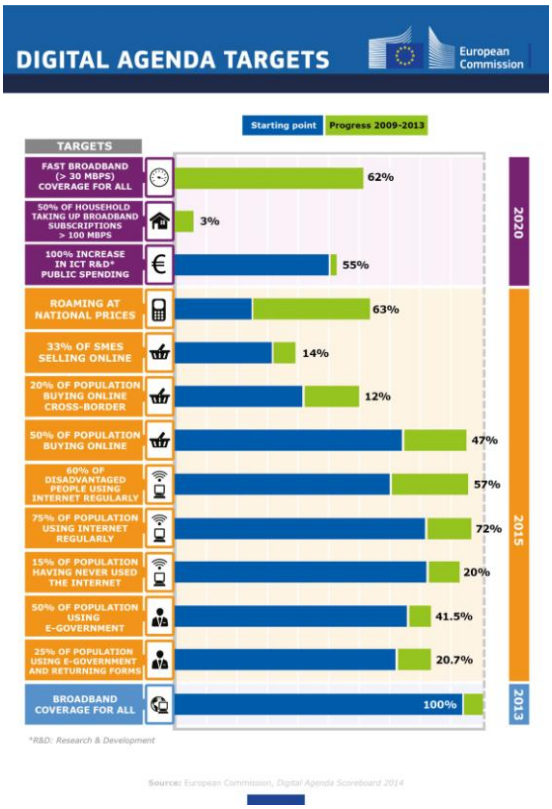

Ilustração 4- Diagrama das metas da Agenda Digital (2013 -2020).

Imagem de http://ec.europa.eu/digital-agenda/en/digital-agenda-scoreboard consultada a 28 de outubro de 2013.

#	*N.º*	*Action*	*«Deadline-Status»*	*Obs./«Link»*
1	28	*Reinforced Network and Information Security Policy*	31/12/2012-Okay	*Key Act. 6*
2	29	*Combat cyber-attacks against information systems*	*31/12/2010-Okay*	*Key Act. 7*
3	30	*Establish a European cybercrime platform*	*31/12/2012/Okay*	*See Act. 31*
4	31	*Analyse the usefulness of creating a European cybercrime centre*	*31/12/2011/Okay*	*EC3*
5	32	*Strengthen the fight against cybercrime and cyber-attacks at international level*	*31/12/2015/Working*	*Cyber Atlantic 2011*[3]
6	33	*Support EU-wide cyber-security preparedness*	*31/12/2015/Working*	*See Act. 39*
7	34	*Explore the extension of security breach notification provisions*	*31/12/2012/Delayed, no repport available*[1]	*See Act. 12*
8	35	*Guidance on implementation of Telecoms rules on privacy*	*31/12/2011/Delayed no repport available*[2]	*ePrivacy Direct. 2010*
9	36	*Support reporting of illegal content online and awareness campaigns on online safety for children*	*31/12/2015/Okay*	*Bett. Internet for Childrens*
10	37	*Foster self-regulation in the use of online services*	*31/12/2015/Okay*	*Idem*
11	38	*Member States to establish pan-European Computer Emergency Response Teams*	*31/12/2012/Okay*	*EU CSS Act.124*
12	39	*Member States to carry out cyber-attack simulations*	*31/12/2010-Okay*	*Cyber Europe*[4]
13	40	*Member States to implement harmful content alert hotlines*	*31/12/2013-Okay*	*Link Act. 36*

#	N.º	Action	«Deadline-Status»	Obs./«Link»
14	41	*Member States to set up national alert platforms*	*31/12/2012/Okay*	*Link Act. 31*
		Ações externas complementares de Digital Agenda Review Packadge		
a	123	*Proposal for Directive on network and information security*		
b	124	*EU Cyber –security strategy (CSS)*		
c	125	*Expand the Global Alliance against Child Sexual Abuse Online*		

Tabela 1 – Ações da Agenda Digital **do Pilar III da Confiança e Segurança**

Tabela adaptada a partir de (http://ec.europa.eu/digital-agenda/en/our-goals/pillar-iii-trust-security) e consultada a 28 de outubro de 2013.

[1]http://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-34-explore-extension-security-breach-notification-provisions, consultado a 18 de junho de 2014.

[2]http://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-35-guidance-implementation-telecoms-rules-privacy, consultado a 18 de junho de 2014.

[3] https://www.enisa.europa.eu/activities/Resilience-and-PICI/cyber-crisis-cooperation/cce/cyber-atlantic

[4]https://www.enisa.europa.eu/activities/Resilience-and-PICI/cyber-crisis-cooperation/cce/cyber-europe/ce2014/cyber-europe-2014-information/briefing-pack

A peça restante do *puzzle* –atual– é a, já introduzida, UE-ECS tornada pública a 07 de fevereiro de 2013 e intitulada *'Cybersecurity Strategy of the European Union:* ***an Open, Safe and Secure Cyberspace****'*, emanada pela *VP/AR*, senhora Catherine ASTHON, e apresentada em conjunto ao PE, ao Conselho, ao Comité Económico e Social e ao Comité da Regiões, (ver Seção **1.6** do **Capítulo 1.**).

Nela, são definidos, em primeiro lugar, os *Princípios para a Cibersegurança* preconizados pela UE: (I)–Os valores nucleares da UE aplicam-se tanto ao mundo físico como ao digital; (II)–A Proteção dos direitos fundamentais, a liberdade de expressão, a proteção dos dados e da privacidade; (III)–Acesso para todos; (IV)–Governação democrática e eficiente em regime de participação multilateral; (V)–A responsabilidade partilhada para assegurar a segurança.

São ainda descritas, em segundo lugar, as *Prioridades Estratégicas e Ações Associadas* por parte da UE: (i)–Atingir a ciber-resiliência, através de uma política coerente e sistemática na área dos RSI, das PICs (incluindo o campo nevrálgico das PICIs), envolvendo uma estrutura de gestão das mesmas –na sua maioria em regime de PPP– partilhada e multilateral, responsabilizando todos os ***stakeholders***(TD&T13), quer nos planos nacionais dos EMs, comunitária ao nível das instituições e agências da UE e no plano internacional. Neste último plano, dever-se-ia aproveitar todas as

oportunidades nos fóruns competentes da ONU, nomeadamente no *IGF* da *ITU*[97], da Organização para a Cooperação e Desenvolvimento Económico (OCDE/*Organization for Economic Co-operation and Development–OECD*)[98], os instrumentos bilaterais entre a União e os outros Mercados instituídos: *North American Free Treaty Association–NAFTA*, *Mercado Comum do Sul–MERCOSUL*, *Association of Southeast Asian Nations–ASEAN*, etc.; (ii)–Reduzir drasticamente o cibercrime, como "o asa" dos RSIs, com a criação do *European Cyber Crime Center–EC3*[135], no seio da *EUROPOL*[134], no CdE, na Assembleia Geral[99] da ONU (*United Nations General Assembly–UNGA*), etc.; (iii)–Desenvolver uma política de Ciberdefesa e as capacidades relacionadas com a PESC, através da AED, procurando a adaptabilidade de tecnologias e procedimentos existentes e utilizados por parceiros da UE e/ou da OTAN, no apoio a ações humanitárias e de segurança da UE a nível internacional; (iv)–Desenvolver recursos industriais e tecnológicos para a Cibersegurança, também, através da AED, procurando incorporar naquela –PESC– as possíveis tecnologias já utilizadas na Ciberdefesa, em particular na vertente defensiva de prevenção e dissuasão; e, (v)–Estabelecer uma política internacional coerente para o Ciberespaço da UE, promovendo os Valores Nucleares da UE nos fóruns internacionais relacionadas com a *IG*.

Em terceiro lugar, são descritos os **Papéis e as Responsabilidades** das várias instituições e agências da UE para a implementação (ver quadro a seguir) e respetivo acompanhamento da UE-ECS para ajustamentos e avaliação.

---

[97] "At the operational level, in recent years the ITU has become a major player by organizing the Internet Governance Forum (IGF), World Conference for International Communication (WCIT), and World Summit on the Information Society (WSIS)." (BENDIEK & PORTER, European Cyber Security within a Global Multistakeholder Structure, 2013, pp. 167-168)

[98] "[…] the OECD has developed a set o principles for a safer Internet[*]. [*].http://www.oecd.org/dataoecd/40/21/48289796.pdf" (BENDIEK & PORTER, European Cyber Security within a Global Multistakeholder Structure, 2013, p. 170)

[99] "At the international level, the UN General Assembly has adopted several resolutions on cybersecurity. The Social and Economic Committee resolution 56/121 'Combating the Criminal Misuse of Information Technology' and 57/239 'Creation of a Global Culture of Cybersecurity' aim to combat the safe-haven problem. Resolution 64/422 'Globalization and interdependence: science and technology for development' asks UN Member States to review their respective capacities to defend against attacks on critical infrastructure. In 2009, the Disarmament Committee adopted resolution 64/386 ' Developments in the field of information and telecommunication in the context of international security', cautioning against state build-up of cyber warfare capacities.[*] The 2010 UN Report on Cybersecurity launched a broad debate on the application of established principles of international law and standards to cyberspace[**]. [*].UN Gen. Assembly, *Report of UN Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security*, A/65/94, 24 (Jun. 2010). [**].CARR, J., *Inside Cyber Warefare, Napping the Cyber Under World c/3* (Beijing u.a. 2010)." (BENDIEK & PORTER, European Cyber Security within a Global Multistakeholder Structure, 2013, p. 167)

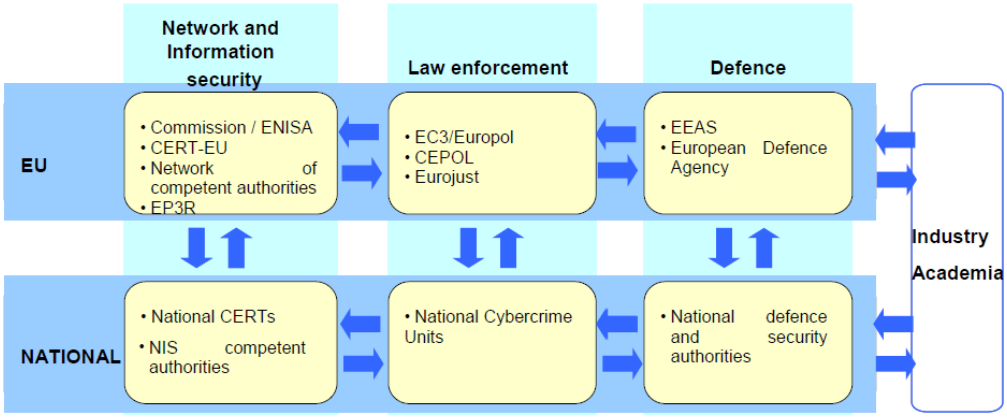

Ilustração 5- Diagrama de Funções/Papéis e Responsabilidades da Estratégia de Cibersegurança na UE.

Diagrama retirado da Estratégia de Cibersegurança para a UE, na p. 17, e consultado a 28/10/2013.

No próximo Capítulo I intitulado, **As Políticas de Segurança do Ciberespaço na UE,** serão descritos os propósitos relevantes de ambas –a Agenda Digital e a UE-ECS– no que diz respeito à situação atual e possíveis desenvolvimentos a curto-médio prazo, de dois a três anos, nomeadamente: O papel da ***ENISA***; **O Pilar III de Confiança e Segurança da Agenda Digital**, sua gênese, dinâmicas e atual "estado-da-arte"; A análise, sintética, dos documentos emanados nas **Estratégias de Segurança do Ciberespaço de EMs** "expressivos" em dimensão da UE, nomeadamente – O Reino Unido, a Alemanha, a França e a Suécia[100]; Analisa-se, também, de forma resumida, o possível **contributo dos EMs de pequena dimensão**, como a Holanda a Estónia e Portugal[101] na definição da Política de Segurança para o Ciberespaço da UE; No final do Capítulo serão abordados **Os Direitos dos Cidadãos, a Privacidade e a Proteção de Dados**. No Capítulo II, analisaremos a possível cooperação ente a UE e a OTAN: **2.1. A procura de Quadros Jurídicos e Referenciais**

[100] Deparou-se difícil consultar informações sobre a Suécia por duas razões: A primeira porque o «link» apresentado no sítio de Internet http://www.cert.org/incident-management/national-csirts/national-csirts.cfm?, aponta para o sítio sueco Sweden CERT-SE Swedish Information Technology Incident Center https://www.cert.se, que não tem informação a não ser em língua sueca, pelo que torna-se difícil analisar o seu conteúdo, ainda que sumariamente. A segunda prende-se com a não existência de uma Estratégia Sueca de Cibersegurança publicada, que seja do nosso conhecimento. Foi encomendando um estudo, à RAND Europe (disponível em http://www.rand.org/pubs/research_reports/RR235.html, consultado a 18/06/2014) e intitulado «Cyber security Threat caracterization: A rapid comparative analysis» sobre questões relevantes para desplotarem a construção de um futuro documento estratégico sobre o assunto encomendado pelo Cabinet Office and Department of Defence, the Swedish National Defence College's Center for Asymmetric Threat Studies (CATS), assim como o estudo (CAVELTY M. D., "A Resilient Europe for an Open, Safe and Secure Cyberspace", 2013)

[101] No mesmo sítio de Internet http://www.cert.org/incident-management/national-csirts/national-csirts.cfm?, quanto ao nosso país existem dois *links*. Um deles aponta para o sítio CERT.PT *Computer Emergency Response Team Portugal* http://www.cert.pt, (tratando-se de uma estrutura nacional de *CERT*, predominantemente de empresas privadas) e o outro, o primeiro e supostamente mais importante, CERT.GOV.PT *Computer Emergency Response Team Goverment* Portugal http://www.ceger.gov.pt, que aponta para o CEGER (que por sua vez tem no seu interior um «link» para dois projetos: um concluído, julgamos ter-se tratado de um «projeto-piloto» designado Disaster-Recovery (www.disasterrecovery.gov.pt , que decorreu entre 1 de setembro de 2009 e 30 de setembro de 2012 e teve como parceiros, para além do CEGER, o Governo das Ilhas Baleares e o Governo de Gibraltar) e um outro projeto, em curso (1 de novembro de 2013 a 30 de outubro de 2015), designado CERTCEGER, que julgamos tratar-se e finalmente, do futuro CERT/CSIRT nacional e oficial de Portugal.

Reguladores; **2.2. Papéis e Responsabilidades das PPPs no Ciberespaço**, em particular ao nível das PICIs; **2.3. As Regras para Ações Militares de Conduta no Ciberespaço**; e, **2.4. Medidas Dissuasoras de Contenção no Ciberespaço** no sentido de poderem ser utilizadas como "ferramentas" de enquadramento e/ou complementares para o binómio UE-OTAN. Para concluir, definem-se recomendações de avaliação sobre "ativos" que interessam à Cibersegurança na UE e sintéticas conclusões relativas ao ponto de situação atual, ao percurso a efetuar e a possíveis desenvolvimentos relacionados com dimensão política da Cibersegurança internacional que poderão ser "moldados" ou influenciados pela UE *per si* ou em cooperação – bilateral ou multilateral – com outras instituições e organizações, rumo à *IG*. Isto, porque, após os fracassos de 2012 na *World Conference on International Communications–WCIC* da *ITU* no Dubai, e *deadlocks* resultantes entre os *BRICSs*, membros da Organização de Cooperação de Xangai (OCX/*Shangai Cooperation Organization–SCO)* e outras duas dúzias de países membros da ONU, por um lado, e os EUA, a UE e os países do designado –*West.*[102]– por outro. Este cenário de "choque" de perspetivas de Governação da Internet (como parte substancial do ciberespaço) e o *deadlock* resultante, foi "catalisado" pelas revelações de 2013 (atrás referidas sobre a *NSA*). Desencadearam iniciativas variadas, que estão em curso, relacionadas com os temas centrais, complexos e controversos subjacentes à *IG* do presente. Por exemplo, a realização: do *Future of Internet Governance–FoIG*, consultar em http://www.internetsociety.org/ e/ou NETMundial (com um dos países impulsionadores – a RFB, consultar em http://netmundial.br/); o incremento do *Internet Governance Project–IGP*, consultar http://www.internetgovernance.org/; ou a *Global Commission on Internet Governance–GCIG* que teve o seu lançamento em Davos-Klosters, Suiça, a 22 de janeiro deste ano –2014– e presidido pelo ex-Ministro dos Negócios Estrangeiros da Suécia, Senhor Carl Built, coordenada por dois Think-tanks de renome internacional: *Centre for International Governance Innovation–CIGI*, (Ca) consultar em http://www.cigionline.org/activity/organized-chaos-reimagining-internet?gclid=CP3c2p_tn8ECFY_MtAodmicA2g e a Britânica, *Chatham House*, do *Royal Institut of International Affairs*, consultar em http://www.chathamhouse.org/about/structure/international-security-department/global-commission-internet-governance-project; (consultadas a 08 de setembro de 2014.) A própria UE[103] também tem essa sensibilidade de que será necessário trabalhar de forma séria e multilateral na *IG*, como de resto se pode verificar em http://ec.europa.eu/dgs/connect/en/content/international-internet-governance-and-management-eu.

[102] (BRZEZINSKI, 2012, p. 8)

[103] "Our vision is to maintain a global model of Internet governance, reformed in line with the principles agreed through a multi-stakeholder process. The principles should allow for Civic responsibility; One internet; Multi-stakeholder governance of the Internet; Pro-democracy; Architecture matters; Confidence of users and Transparent governance."

Capítulo I - As Políticas de Segurança do Ciberespaço na União Europeia

> "During the next three years [2013-2015], cybersecurity-related discussions in Europe will take up issues that are currently being discussed and addressed in the United States. The discussions must engage society at all levels because cybersecurity affects society at all levels." (SALONIOUS-PASTERNAK & LIMMÉIL, 2012, p. 7)

> "But the fact is the growing number of incidents every day. It is estimate that more than a million cyber attacks are been make every day and is growing. So we need to make sure that our citizens can benefit from an open, safe and free Internet. And we can do that if only we have a secure environment. […] If we want to be credible in our efforts, we need better legislation; we need more resources and overall more coordination. We had advanced quite a lot but we need much more. One initiative that I had presented than two years ago is now a legal proposal for clear and harmonizes rules to reduce cybercrime with high sanctions at major offenses. This is now been negotiated and I hope soon finalized between the Council and the European Parliament." Commissioner MALMSTRÖM, Cecilia in charge for Home Affairs on Press Conference about European Union Cybersecurity Strategy in Brussels – 07 de fevereiro de 2013, consultado em 07 de abrirl de 2014.

Como se pode aferir (mesmo não se prestando muita atenção), pelas notícias do quotidiano que são emanadas por diversos canais –televisão, imprensa em papel e digital, blogues, redes-sociais e até pela rádio– os incidentes de Cibersegurança que trasvazam para a comunicação social são, em número e gravidade, significativos, mesmo em Portugal[104] –cujo número de info-excluídos é significativo, mesmo, ao nível do senso comum. A primeira razão daquele significativo incremento deve-se, sobretudo, à interatividade e crescente migração do chamado "mundo-real" para o admirável

[104] "Há um mês e meio [março de 2011], Portugal sofreu um ataque informático a partir principalmente de servidores da China e da Rússia. Os pedidos de acesso ao domínio de topo português – **.pt** – foram de 20 mil por segundo, afirma/[afirmou] Pedro VEIGA. O Presidente da Fundação para a Computação Nacional (FCCN) usou o ataque esta manhã, no âmbito da conferência 'Cibersegurança: do pensar à ação', realizada pelo Gabinete Nacional de Segurança (GNS), Eurodefense Portugal e Associação para as Comunicações e Eletrónica das Forças Armas (AFCEA), para exemplificar que Portugal não está imune a ciberataques." A 03/mai./2011 em http://www.computerworld.com.pt/2011/05/03/portugal-sem-estrategia-coordenada-de-ciberseguranca/ , consultado a 10/jun./2014.

mundo novo[105], ou "Cibermundo" em geral associado ao Ciberespaço, e para a Internet em particular. Em segundo lugar, como resultado, ainda insipiente, é certo, de sensibilização, onde «[Os] Cidadãos tornaram-se, ainda mais, despertos para os riscos *on-line*, e também ainda mais relutantes em confiarem nas ferramentas disponíveis, igualmente, '*on-line'* para sua proteção.» Referia-se a senhora Comissária KROES –a 12 de março p.p. em Estrasburgo– que tem vindo a ser feito um alerta generalizado para os possíveis perigos inerentes à utilização dos mesmos, cibermundo e Internet, resultantes: do aumento de situações de espionagem –roubo de propriedade intelectual; pirataria e contrafação de produtos através de *eCommerce*; extrusão de valores –através de *sites* fraudulentos, aparentemente idênticos aos legítimos; roubo de identidades e utilização de *Cyber-personae*; *E-mails* abusivos e ilegítimos –*Phishing*[DT&T09] *e Spear-phishing*[TD&T10]) através de Engenharia Social; invasão de privacidade –controlo remoto e abusivo de *web* câmaras e de microfones[126]; e, negações de serviço distribuídas, –*Distrtibuted Denial of Service–DDoS*[TD&T11] ou não, *Denial of Service–DoS*[TD&T12]– de acesso a *Sites*, etc. Se migrarmos de Portugal–PT para o espaço europeu em geral, ou para a UE em particular, estes fenómenos passam a ter uma outra importância, pelo sentido de cidadania mais acutilante –nomeadamente, nos EMs do centro e norte da Europa–, pelo nível de alfabetização elevado e o nível de infoexclusão reduzido ou insignificante, mesmo em faixas etárias média-altas. Por estas razões, não será de espantar que estes temas tenham suscitado, nos últimos anos e com particular incidência, nos últimos meses, debates diversos –nas organizações da sociedade civil, na Academia e até ao nível governamental dos EMs e institucional na União, nomeadamente no PE. Foram catalisados pelas, já atrás mencionados, denúncias de vigilância generalizada, dos ataques informáticos a países amigos e/ou aliados, ou a empresas, por parte de serviços secretos americanos e europeus "afins", porque «[n]os documentos expostos por SNOWDEN, ficou claro que o Britânico *GCHQ* não é só o parceiro mais próximo e altamente capaz mas um subsidiário pago pela *NSA*.» (MASCOLO & SCOTT, 2013, p. 5) Isto, para já não falar em ataques de países terceiros a organismos e empresas da União, dentro e fora da UE. Neste Capítulo, iremos abordar de forma mais direta: A renovação de mandato da *ENISA* (até 18 de

[105] "In short, we stand on the threshold of a new world, much as we did in 1945 [after the first atomic bomb was exploded]. From this vantage point, nobody can say where the future might lead. But we do know that the changes that lie ahead will affect everyone on the planet. (ROSENZWEIG, 2013, p. 7)

junho de 2020); As suas relações institucionais no âmbito da UE e nas parcerias Público-Privadas do MUE. Com particular acutilância, devido ao necessário crescimento, do MDE, que foi, é, e continuará a ser o *leitmotif* da criação e implementação da Agenda Digital. Nesta, interessa-nos os domínios da Confiança e Segurança e a possível consolidação da UE-ECS, muito em particular, quando relacionada com a PESC e a PCSD, «como parte integral daquela e que compreende uma dimensão externa da UE, estendendo-se para além da dimensão militar;» (NUNES, 2012, p. 1) Convém, de igual forma, analisar qual o enquadramento da PESC com organizações internacionais, particularmente e para o objetivo deste trabalho, com a *OTAN*. Mais propriamente, as relações com o *CCD CoE* –que é conhecido na gíria, «com o nome de código, ***K5*** porque aparece cinco vezes a letra **k** no seu nome original, '***K****über****k****aitse* ***K****ompetentsi****k****es****k****us*'» (LAASME, 2012, p. 16)– de Tallinn, na Estónia e com a estrutura de Comando e Controlo de Ciberdefesa da OTAN.

1.1 A Agência Europeia para a Segurança das Redes de Informação (ENISA)

> "Em 2004, o Parlamento Europeu e o Conselho adotaram o Regulamento (CE) n.º 460/2004[LRG06] que cria a ENISA a fim de contribuir para a realização dos objetivos consistentes em assegurar um elevado nível de segurança das redes e da informação na União e desenvolver uma cultura de segurança das redes e da informação em benefício dos cidadãos, dos consumidores, das empresas e das administrações públicas. Em 2008, o Parlamento Europeu e o Conselho adotaram o Regulamento (CE) n.º 1007/2008[LGR18] que prorroga o mandato da Agência até março de 2012. O Regulamento (CE) n.º 580/2011[LGR33] prorroga o mandato da Agência até 13 de setembro de 2013." (9) do preâmbulo do Regulamento (UE) N.º 526/2013[LGR105] do Parlamento Europeu e do CE de 21 de maio de 2013
>
> "A Agência é criada por um período de sete anos, a contar de 19 de junho de 2013." Artigo 36.º do Regulamento (UE) N.º 526/2013[LGR105] do Parlamento Europeu e do CE de 21 de maio de 2013
>
> "For us, we will see a great success because the European Parliament, the European Council and the Commission it will extend our tasks and also our responsibilities […] The good thing is for the first time different perspectives are put together. So, you had Commissioner/[Vice-President] KROES [in charge for *Digital Agenda*], [Commissioner] MALMSTRÖM [responsible for the Citizen Rights] , you had [Vice-President & HR] ASTHON from the *Foreign Action Service* which give us together, to put together the *Digital Agenda* and the Internet Security and all of aspects of Europe. And the interesting thing is, different Agencies got different tasks and us for the future. The EUROPOL, ENISA, the EDA/[European Defense Agency] and you have the research area. So, this means ENISA will work more together with other agencies in this area." (HELMBRECHT, 2013) acedido em

http://www.vieuws.eu/citizens-consumers/cyber-security-udo-helmbrecht-enisa/ a 10 de março de 2014.

Sua génese e afirmação como "A Agência" da União Europeia

A *ENISA*, ou como é designada na gíria "a Agência", –tal é a sua importância, quanto ao peso considerado do domínio de operação e crescente âmbito de intervenção– , se assim podemos dizer, aplicou a expressão latina: *veni, vidi, vinci*. Vê pela quarta vez reafirmada a extensão do seu mandato – desta vez, até meados de 2020 –emanado em conjunto pelo PE e pelo Conselho. Por esta razão, poder-se-á inferir que as relações institucionais entre a *ENISA* e as instituições de topo da UE são "cordiais", em especial com o Conselho. O mesmo já não se poderá dizer do PE, devido à pluralidade ideológica e à variedade de sensibilidade e *lobbies* das comissões que abordam assuntos relacionados com a Cibersegurança. A *ENISA* quando é criada em 2004 era um "embrião" do que é hoje. Começou por ser um mero projeto-piloto[106] –cujo enfoque era a pesquisa/investigação com a Academia, o desenvolvimento e a assessoria– que, com o decorrer dos seus mandatos, singrou e ocupou um espaço que é seu por direito próprio. No entanto, a transformação não acontece por acaso, mas devido, pensamos nós, a três razões: A primeira, pelo trabalho meritório da equipa de gestão, nomeadamente do seu –atual e segundo– presidente executivo, Doutor Udo HEMBRECHT –o primeiro Presidente Executivo, de 2004 a 2009, foi o Senhor Eng.º Adreia PIROTTI[107]–,

[106] "The European Network and Information Security Agency (ENISA) is an EU agency supervised and financed by the European Commission DG INFSO[/DG CONNECT]. Originally set up in 2004 as an advisory body for the Member States and EU institutions in network and information security issues, ENISA has rapidly established itself as an actor in the European cybersecurity community. Until 2009 the ENISA mandate only allowed it to function as a research body, although it was able to support a number of Member states in advising on operative matters (including how to set up a CERT). Member states agreed in 2009 to extend ENISA's mandate and resources; however, how exactly the role of ENISA will be expanded in the future is still a matter of deliberation. The new ENISA mandate is currently still under review, but in effect it formalizes many of the new roles that ENISA already assumed in 2010, such as coordinating Pan-European exercises and facilitating discussions with the private sector. Further to that, the current proposal entails that ENISA would also set up a CERT for EU institutions and assume the associated responsibilities as defined in Article 13A of the revised Telecommunications Framework Directive. Also, ENISA will be responsible for the European Information Sharing and Alert System (EISAS) which, potentially, could play a major role in improving European cybersecurity. It is expected that ENISA will play a stronger role in overseeing the security aspects of the EU telecommunications' sector. It will include the Internet Service Provider's mandatory incident reporting and the requirement for the Member States to apply appropriate risk management measures to ensure the level of services, and, if advised so by ENISA, the Commission may mandate Member state to adopt technical measures based on international standards for communication network security. " (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 34)

[107] Entrevista dada ao *chapter* da *Information Systems Audit and Control Association – ISACA* de Roma e publicada no seu número 9 de dezembro de 2004. "On 6th October [2004], Adreia Pirotti was questioned, evaluated and then confirmed by Te European Parliament as Executive Director of ENISA,

consubstanciado pelo trabalho profícuo, em conteúdo e oportunidade, e expressivo –devido ao considerável número de publicações pertinentes e publicamente disponíveis–, com impacto no campo da Cibersegurança. Também, das equipas[108] técnicas e administrativas das várias áreas de atuação –*CERT*s, PICIs e Resiliência, Identificação e Confiança e a de Avaliação de Riscos– ver o menu horizontal, no canto superior direito, do sítio web "oficial" público da *ENISA*;

Ilustração 6- Imagem parcial do sítio web da ENISA da UE.

Fonte (http://www.enisa.europa.eu) consultado a 04 de junho de2014.

A segunda, devido ao incremento do "peso" dos assuntos relacionados com a dimensão política da segurança do Ciberespaço nas agendas da UE[109] e na política internacional[110]; e, a terceira, decorrente da realidade pertinente das organizações e das empresas face ao crescendo de ocorrências de intrusão, roubo de propriedade intelectual, tendo como consequência avultadas perdas financeiras, da necessidade de colocar mais serviços e produtos disponíveis no Ciberespaço para fazer face à crescente procura, à enorme concorrência –muitas vezes desleal pelas razões de intrusão, fraude e

---

the European Network and Information Security Agency. He is currently the only Italian Director out of the sixteen European agencies. […]" Consultado em http://www.isacaroma.it/pdf/news/0412-isacaroma-news.txt a 06/jan./2013 .

[108] "[…] ENISA has 62 personnel [em 2011] based at its headquarters in the island of Crete. ENISA staff can undertake missions to locations across Europe (and further afield). ENISA also provides a Mobile Assistance Team to serve Member States. We were told that there are three members of staff at ENISA who work in, but are not uniquely dedicated to, cybercrime. ENISA has established a role for itself as a trusted intermediary to the European Computer Emergency Response Team (CERT) community." (RAND Europe, 2012, p. 93)

[109] "In 2005, the landmark Council Framework Decision on Attacks against Information Systems[(i)] was adopted, which required all Member States to introduce legislation (by 2007) to deal with the principal types of cyberattacks, and, most significantly, which provided common definitions for such attacks." [(i)] Council Framework Decision on attacks against information systems, 2005/222/JHA, 24 February 2005, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193_en.htm. [(LRG07)]

[110] "Without a doubt, cyber-security is the policy-issue of the hour. The cyber-attacks on Estonia in 2007, the discovery of Stuxnet[TD&T01], the industry-sabotaging super worm[DT&T02] in 2010; numerous instances of cyber-espionage, culminating in the Snowden revelations this year; and the growing sophistication of cyber-criminals as evident by their impressive scams have all combined to give the impression that cyber-attacks are becoming more frequent, more organized, more costly, and altogether more dangerous. In short, cyber-threats and the measures necessary to counter them are considered a top priority in more and more states around the world, including many European countries." (CAVELTY M. D., "A Resilient Europe for an Open, Safe and Secure Cyberspace", 2013, p. 3)

roubo–, em suma à Globalização e às suas inevitáveis consequências no Ciberdomínio, Cibercrime e Ciberespionagem.

Funcionamento, relações institucionais na União Europeia e internacionais

A *ENISA* opera, de forma indireta, em todos os EMs por iniciativa própria, normalmente em parceria com aqueles ou quando solicitada pelos mesmos[111]. Tem a sua sede em Heraklion, na ilha Grega de Creta. É aqui que estão sedeadas a investigação e desenvolvimento, a gestão financeira e administrativa, informática e das infraestruturas, os recursos humanos, a formação, a comunicação e os assuntos públicos, a relação com instituições internacionais, como a OTAN e o seu *CCD CoE*–'***K5***' , o *IGF* da *ITU* pertencente à ONU, a *Internet Engineering Task Force–IETF*, a *International Electrical and Electronic Engineering–IEEE* e a *Wold Wide Web Consortium–W3C*. Foi criado um gabinete na área metropolitana de Atenas por razões de prontidão logística dos *CERT*[112] e para apoio a operações relacionadas com outros domínios operacionais da Agência e da UE a fim de melhorar a sua eficiência.

A *ENISA* é constituída por um conselho de administração, composto por um elemento efetivo e um suplemente de cada EM. Por razões de eficiência, é constituída em cada mandato, uma Comissão Executiva que poderá reconduzir elementos da anterior, e um diretor executivo, já referido, assim com, restante pessoal do *staff* de suporte um Grupo Permanente de partes Interessadas (GPpI/*Permanent Stakeholders Group–PSG* ou ***stakeholders***[113] [114]). Este grupo tem uma importância significativa

[111] "ENISA's relationship with Member States in relation to cybercrime are mainly through the Management Board (MB) and National Liaison Officer (NLO) networks, and through events co-organised with the Member States. We were told by ENISA that cybercrime is sometimes a main theme at these events, but 'is a constant element in the discussion of network and information security."

[112] "A major element of ENISA's work is the support it provides to CERTs, and ENISA's Work Programme for 2011 includes an activity called 'Good Practice for CERTs to address NIS aspects of cybercrime' which is likely to be continued in 2012. This activity aims to improve CERTs' capability in addressing NIS aspects of cybercrime. The outputs from this work will be a good practice guide for CERTs in addressing NIS aspects of cybercrime and ENISA's sixth workshop for CERTs in Europe. […] ENISA has been active in helping to develop her concept of national/governmental CERTs and supports the CERT community in a variety of ways. ENISA could play a role in bringing together organizations working in NIS, such as CERTs, with organizations directly working in cybercrime, to share good practice and establish dialogues. ENISA has embarked upon facilitating activities to reinforce co-operation between national/governmental CERTs. These activities (such workshops, exchange of best practice and training) include measures to improve co-operation at national level between national/governmental CERTs and LEAs." (RAND Europe, 2012, pp. 93-94)

[113] "The agency can be described has an European centre of expertise in the cybercrime field. Concerning the organizational structure, the agency is composed by a management board, an executive director and a

crescente, devido, como já vimos, a que nas democracias "ocidentais" grande parte, ou mesmo a quase totalidade, das PICs e das PICIs –de informação– estarem ou pertencerem a organizações ou empresas –muitas, transnacionais– do domínio privado, ainda que em regime ou «modelo de PPP adaptado»[115] no caso das PICs (CAVELTY M. D., "A Resilient Europe for an Open, Safe and Secure Cyberspace", 2013, p. 4).

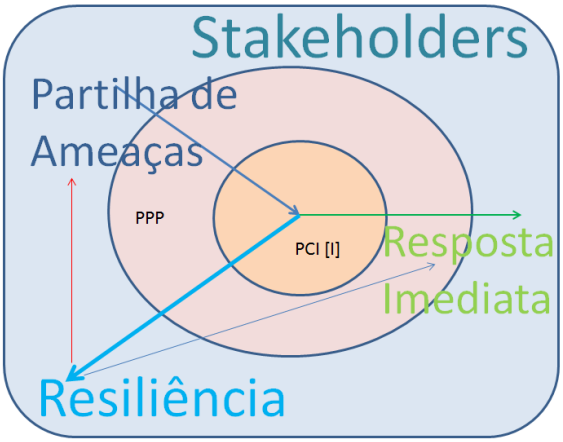

Ilustração 7- Diagrama –do autor baseado em (CAVELTY M. D., 2013)– sobre a ação de Resiliência.

1.2 O PILAR III de Confiança e Segurança da Agenda Digital

> "Only 12% of European web users feel completely safe making online transactions. Threats such as malicious software and online fraud unsettle consumers and dog efforts to promote the online economy. The Digital Agenda proposes a number of practical solutions, including a coordinated European response to cyber-attacks and reinforced rules on personal data protection." Retirado de (http://ec.europa.eu/digital-agenda/en/our-goals/pillar-iii-trust-security) a 14/jan./2014.

> "Following the successful vote* on the NIS directive on cyber security today in [EP/PE] Strasbourg, Vice President Neelie KROES said [on 13th march this year]: This vote today is very positive news for European citizens, and I would like to thank

Permanent Stakeholders Group (PSG). Moreover, ENISA has the possibility of creating *ad hoc* working groups in specific matters. Another part of ENISA structure is the National Liaison Officers network (NLOs)." (NOTO, 2013, p. 8)

[114] "ENISA has strong links with the public *and* Private sectors. ENISA interacts with the private sector in the field of cybercrime through expert working groups with NIS aspects of cybercrime. ENISA describes itself as having 'well established relationships with relevant stakeholders both the public and the private sectors'."

[115] "2.2. The limitation of a miracle solution – However, difficulties have surfaced in recent years in terms of realizing forms of cooperation that are sometimes due to practical, sometimes to conceptual matters. The core problems are, first of all, that the term 'PPP' can only describe the nature of exiting partnerships in a vary rudimentary way, and the majority of so-called PPP in CIP are not really PPP at all;" (CAVELTY & SUTER, "Public-Private Partnership are no silver bullet: An expanded governance model for Critical Infrastructure Protection", 2009, p. 3)

> the Rapporteur, Andreas SCHWAB, for his hard and efficient work, as well as everyone who has worked on this report. Member States need to be ready to address cyber attacks. Today there are gaps in some countries and we need to fill them. **We are only as strong as the weakest link!** Let's work together to show that governments and lawmakers are part of the solution to online trust – not part of the problem. Now we must all engage closely with the Member States, make sure that they realise the importance of this issue, and aim for a final agreement by the end of 2014. But speed should not be at the expense of substance. People need to regain trust in technology, with the legal safeguards that protect their interests. **My ambition is to make Europe the world's safest online space.** I hope that the European Parliament and national Governments share this ambition." A 13/mar./2014.
> [*]521 in favor; 22 against; 25 abstentions. Consultado em http://ec.europa.eu/digital-agenda/en/news/great-news-cyber-security-eu-european-parliament-successfully-votes-through-network-information a 04/jun./2014.

Desconfiança na Privacidade do Cidadão face à Internet

A confiança do cidadão europeu em relação à segurança dos serviços disponibilizados no Ciberespaço por empresas de serviços, lojas *on-line*, sítios de organizações públicas, na Internet, dos EMs, assim com, nos sítios institucionais da UE é, ainda, baixa, como provam os números do último Euro-Barómetro de 2013[116]. Isto, apesar da chamada Agenda Digital já se encontrar em implementação desde, praticamente, o início de entrada em funções da CE–"Barroso-II", que este ano cessa responsabilidades, i.e. desde 2009, por isso, há cinco anos. Aliás, poder-se-á constatar que o suporte formal para, por exemplo, a '***Ação 28–Reforço das Políticas de Segurança para as Redes e Sistemas'*** –assunto referenciado com *RSI*, que na gíria da UE, como já referido, é sinónimo de Cibersegurança–, só passou no PE, no passado dia 13 de março de 2014 e sem unanimidade –ver a introdução da seção.

O porquê da importância da ***Ação 28***? (ver Tabela 1, pp. 31-32) Esta ação, em concreto, permite um reforço da política de proteção de RSIs, através do incremento de autoridade dado à *ENISA* –cujo processo de recondução de mandato por mais sete anos é sintomático–, assim como, uma maior amplitude do seu campo de intervenção. Mostra, preocupações operacionais de sobreposição de agências. Induz, também, alguma inabilidade, desconhecimento, ou mesmo, uma certa displicência das instituições da União para lidarem com os assuntos relacionados com RSIs, na articulação entre Ciência Política e Tecnologia. Isto pode denotar, *a priori*, uma falha na formação –possivelmente resultante da insuficiente abrangência dos currículos– para

[116] Consultar: Relatório em http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf ; e Factsheets em http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_fact_pt_pt.pdf, consultado a 21/ago./2014.

novas áreas de desenvolvimento humano, como é o caso do Ciberespaço. Espelha, de igual modo, a necessidade de harmonização de procedimentos em todos os EMs da União, uma vez que, o que aqui interessa, é melhorar «os elos mais fracos» do sistema, (será que, entre eles não se encontrará o nosso País?) –Ver a Seção **1.4. O papel dos estados membros de pequena dimensão na definição da Política de Segurança para o Ciberespaço da UE** e as **Recomendações e Conclusões**. Conduz, na mesma linha, os parceiros a adotarem padrões normalizados, considerados minimamente aceitáveis para a segurança coletiva do MDE no Ciberespaço da UE. Induz, igualmente, os membros a instituírem, legal e formalmente, os *CERT* nacionais e o *CERT-EU* e a coloca-los operacionais, por forma a estarem 100% funcionais e com a sua estrutura e dependências definidas. Obriga, também, os seus recursos humanos a serem devidamente recrutados, qualificados, treinados através de ciber simulações ou exercícios[117] e, acima de tudo, atualizados em relação ao panorama, altamente, cinético e volátil da Cibersegurança. Poderá, de forma pró-ativa, preparar as empresas e organizações que o solicitem, ajudando-as contra, possíveis, ciber ataques. Esta medida de implementação de *CERT* nacionais e institucionais da UE, da ***Ação 28***, está diretamente relacionada com a '***Ação 38–Os Estados membros para estabeleceram Equipas de Resposta a Emergência Computacional Pan-europeia***' e efetuarem os ciberexercícios Pan-europeus (*Cyber-Europe 201x: x=2010, 2012, 2014, etc.*) de teste e ajustamento da '***Ação 39–Permitir que os Estados membros possam levar a cabo ciberataques simulados***.' Estas duas ações estão também intrinsecamente relacionadas com os conceitos de multiplicidade de interesses dos atores –«a política de Cibersegurança de estrutura de enquadramento a vários níveis e interesses múltiplos[118]»– vitais, devido a grande parte da infraestrutura do Ciberespaço pertencer, em termos de gestão e funcionamento –como vimos–, ao domínio privado da economia, Isto, em virtude da tendência, dos anos 80/90 do século passado, de transferir para esse

[117] "[…] I should say that when we came to the national defence & national security the successful national cyber defence model is already a multi-stakeholder model. It has to be a civilian and military cooperation that is based on it. It should have involvement by the private sector, it should have support of broad civilian base and possible the best advice would be to have good national exercises with all the different national agencies and organizations involved and star doing this often almost as possible in cyber and then a model comes together. So, if you are looking for an advice in this national part." (TIIRMAA-KLAAR, 2013)

[118] "The Multi-Level and Multi-stakeholder Structure of Cyber Security Policy [approach] – In practice, cyber security policy has thus resorted to the 'multi-stakeholder' model, where any group with the relevant expertise (businesses) or the required political authority (states) may participate in the policy-shaping process." (BENDIEK, "European Cyber Security Policy", 2012, p. 19)

setor serviços, até então disponibilizados pelo setor público, nos EUA e na Europa, e tendo por base as chamadas PPPs. Isso, devido à insuficiente disponibilidade financeira do setor público em investimento e manutenção, assim como, suposta melhor gestão, por parte de entidades privadas de serviços públicos, mesmo os considerados estratégicos e essenciais, o que segundo alguns autores é problemático[119].

A razão de ser, do reforço das RSIs, prende-se também com a '***Ação 29Combater os Ciber Ataques contra os sistemas de Informação'*** e apoia a '***Ação 32–Robustecer a luta contra o ciber crime e ciber ataques no plano Internacional'***, assim como, com a '***Ação 33–Suporte à preparação alargada de UE no domínio da Cibersegurança'***, que está diretamente ligada à '***Ação 39–Permitir que os Estados membros possam levar a cabo ciberataques simulados'***. Isto, para uma preparação de futuros ataques reais que poderão contribuir decididamente para serem detetadas falhas funcionais e anomalias organizacionais, processuais e ausência de competências dos recursos humanos adstritos às equipas técnicas responsáveis de gestão, aos *CERT*, e às equipas forenses digitais, consolidando a vital capacidade de Resiliência. Esta, como vimos, é uma importante capacidade dos "Sistemas" de, no mais curto espaço de tempo, voltar a uma situação de funcionamento normal, no extremo e, se possível, regressar à posição inicial que o sistema detinha antes do referido ataque.

A natureza Insegura da Internet[120] e do Ciberespaço

Tudo isto, prendendo-se com a natureza da génese da atual Internet, «base alargada» do Ciberespaço, «em que o enfoque era[/é] numa comunicação rápida, precisa e efetiva –excluindo outros fatores, como, eram os casos, da segurança e da verificação da identidade. [«A Internet não foi desenhada requerendo identificação.» (ROSENZWEIG, 2013, p. 21)]– tornou o Ciberespaço um lugar perigoso» (ROSENZWEIG, 2013, p. 19). «Como inicialmente concebida, a sua única função foi a de transmitir informação a longas distâncias e de forma rápida. Isto fazia todo o sentido quando só havia quatro nós na Internet, e todos qua a usavam conheciam-se uns aos

[119] "[…] that the interests of private business and of the state are often not convergent when it comes to CIP and that PPP are therefore hardly suitable as solutions;" (CAVELTY & SUTER, "Public-Private Partnership are no silver bullet: An expanded governance model for Critical Infrastructure Protection", 2009, p. 3)

[120] "[...] is pervasively insecure, because it was never built with security in mind." (CAVELTY M. D., "The militarisation of cyber security as a source of global tension", 2012, p. 103)

outros,» (ROSENZWEIG, 2013, p. 21). Esta baseou-se em dois princípios: a redundância da distribuição de «pacotes»; e, a necessidade de velocidade na entrega dos mesmos [relativa à tecnologia da época]. Não havia qualquer preocupação com os assuntos de segurança, em particular, com a integridade, a confidencialidade e, também, a autenticidade (*Confidentiality, Integrity and Authenticity*[121]*–C-I-A*) dos pacotes comutados através de circuitos público-privados/dedicados. Naquela altura, quem tinha acesso aos pacotes, eram membros da Academia e/ou das instituições militares dos EUA, em projetos de investigação aplicada e útil a ambos os universos. Não nos devemos esquecer que a atual Internet, nasceu em plena "Guerra-fria" e uma das principais aplicações militares da, então designada, *Advanced Research Projects Agency Network–ARPANET*[122], era a implementação de uma rede de comando e controlo dos instrumentos de deteção e resposta a, possíveis, ataques estratégicos de caráter nuclear. Logo, deveria permitir redundância de transmissão –fiabilidade contra possíveis falhas de unidades atacadas e tornadas inoperacionais– mas, ao mesmo tempo, com uma velocidade compatível com o tempo de reação e a tecnologia então existente. Os circuitos eram, para todos os devidos efeitos, "privados", mesmo utilizando seções da estrutura pública de comunicações, devido ao número de utilizadores ser restrito. Este tipo de arquitetura conduziu a um conjunto de, pelo menos, cinco vulnerabilidades de perigosidade de acesso e ao nível da utilização da atual Internet/Ciberespaço: 1–A facilidade de ações instantâneas e à distância, em que um clique num rato ou numa tecla, efetuados, por exemplo, na Europa, podem provocar uma série de ações sequencialmente programadas e nocivas no extremo da Ásia ou, em qualquer lugar do planeta –ou ao redor dele, por exemplo, num satélite ou estação orbital internacional. «A história da interação humana é, essencialmente, de incrementação da distância. Nos primórdios, atividades, tais, como conflitos armados, vendas de bens, atos malévolos, e

[121] "Independentemente de taxonomias mais elaboradas quanto aos objetivos dos ataques, estes, maioritariamente, na sua essência, significam perverter a informação, ou melhor, as suas propriedades[1]: confidencialidade, integridade e disponibilidade. [1]De modo mais generalizado são reconhecidas três propriedades. No entanto existem outras, ainda que não consensualmente aceites, a de não repúdio e autenticação." (CALDAS & FREIRE, 2013, p. 3)

[122] "In 1966, the Advanced Research Projects Agency **(**ARPA**)** hosted a program with several research institutions called Resource Sharing Computer Networks. ARPA's goal was to link different computers together, both to increase overall computer power and to decentralize information storage. The U.S. government wanted to find a way to access and distribute information in the case of a catastrophic event, such as a nuclear attack. If a bomb hit an important computer line, information transfers would stop immediately. But if there were a way to network computers, other parts of the system could keep running even if one link were destroyed. […]" http://computer.howstuffworks.com/arpanet.htm/printable Consultado a 19/jun./2014.

espionagem requeriam proximidade física.» Ao longo do tempo, esta necessidade foi diminuindo. «No campo de batalha, por exemplo, passou-se da utilização de armas com lâminas [espadas, lanças, baionetas], para arcos e flechas, canhões fixos e artilharia, aviões, e misseis balísticos intercontinentais»[123]; 2–As Assimetrias em arquitetura, infraestrutura e custos de operacionalidade, permitem que «a manipulação de bits e bytes não requeiram o desenvolvimento de uma base industrial sofisticada, nem investimento financeiro substancial. Por outras palavras, as barreiras de entrada no Ciberdomínio são incrivelmente baixas[124].» Aliás se há duas ou três décadas, para aceder à rede pública de comunicações telefónicas, tínhamos que nos registar no operador «local/regional/ou nacional» que detinha toda a infraestrutura física de ligações e pagar uma mensalidade de utilização, hoje basta-nos ter um telemóvel, *tablet* ou portátil com uma antena *Wireless Fidelity–Wi-Fi* (da *Wireless Fidelity Foundation*– tecnologia *IEEE* 802.11) e ir a um *hot-spot* para temos acesso à Internet de forma rápida, fácil e, na maior parte das vezes, anónima; 3–Ao Anonimato e difícil atribuição[125] de ações maliciosas, deve-se referir que a «identificação não é absolutamente impossível de ser determinada, mas sendo, sim, extremamente difícil de

[123] "The Internet is a quantum leap beyond that capability. Now, action in the cyber domain occurs at the speed of light and crosses immense distances almost instantaneously. From your desktop, you can access a website in Japan, read a South American Newspaper, or make a reservation at a restaurant in Paris. But what is easy for you from your home computer is equally easy for any malicious actor in the world who wants access to a computer, say, in America. Whether the object is warfare, terrorism, espionage, or crime, it is no longer necessary for malevolent actors to be anywhere near the venue of their actions." (ROSENZWEIG, 2013, p. 19)

[124] "Further, the structure of the Internet is such that, at least today, offence is much more effective than defense. AS everyone knows, it's almost impossible to avoid a virus infection on your computer. Firewalls and intrusion detection systems [IDS] are only so effective [atualmente já existe a tecnologia *Security Information Executive Management–SIEM*[TD&T13] *e análise de Big-Data*[TD&T14]]. That means that a small group of actors in cyberspace can have an increasingly large effect. A handful or intelligent hackers can compete in cyberspace against the most powerful nations in the world. The group known as Anonymous, for example, has taken down the CIA website and stolen internal e-mails from sophisticated security companies. […] Another way of looking at the problem of asymmetry is through the prism of national security. In the physical world, a country's power is judged by its force of arms. Few other countries can ever come close to wielding the same nuclear power as the United States, for example. But the asymmetry of information power on the Internet changes that dynamic. Such countries as North Korea and Iran are perfectly capable of challenging and perhaps even dominating America in cyberspace. The limits lie in a nation's industrial base or the size of its economy but solely in the intellectual capabilities of its citizens." (ROSENZWEIG, 2013, p. 21)

[125] "The lack of identification – what's called the problem of attribution – is one of the fundamental difficulties of the network. Not only does it create the difficulty of defending yourself from unknown attackers, but it also raises a barrier of effective cooperative action with people or entities that you might actually want to work with, such as your bank. […] One reason identity thieves are almost impossible to deter is that their own identities are almost impossible to discovery. Here again, the contrast with the physical world is remarkable. The requirement of physical proximity to commit a crime means that there are many opportunities to discover the perpetrator's identity – fingerprints, license-plate numbers, and so on. This is not true on the Internet." (ROSENZWEIG, 2013, p. 22)

atribuir, como foi o caso de ciberespionagem, conhecido, por ***GhostNet***[126], que levou mais de um ano, após inexcedível trabalho forense para a identificação da fonte de intrusão,» havendo, no entanto, autores que preconizem, uma outra estratégia de abordagem à atribuição de responsabilidades dos ciberataques, como a atribuição política[127], que é o caso de HEALEY, Jason –antigo oficial da Força Aérea dos Estados Unidos da América–*USAF* e Diretor da Casa Branca para as PIC[I]s e '*Director of the Cyber Statescraft Initiative on The Atlantic Council*'; para mais detalhes ver 13':45" http://www.atlanticcouncil.org/events/webcasts/webcast-cyber-conflict-and-war-yesterday-today-and-tomorrow, consultado a 11 de fevereiro de 2014; 4–A Ausência de Fronteiras na sua grande parte, concretamente, na chamada «camada lógica», pois «não há postos de controlo na Internet. Múltiplos pacotes de dados ou mesmo uma simples mensagem de *E-mail* atravessa múltiplas fronteiras, mas não há, forma fácil, de controlar a passagem e, muito menos de, inspecionar o respetivo fluxo de informação[128];» e, 5–A dificuldade de distinção ou natureza do conteúdo ao nível da sua camada lógica, onde as cadeias de «zeros e uns são todos iguais», não permitindo identificar seja o que for, a quem quer possa ter a veleidade de monitorizar o tráfego[129]. Embora as tecnologias de

126 "An APT[TD&T15] called GhostNet was found in March 2009 in the computers operated by the offices of the DALAI Lama. […]It took an information warfare organization in Canada more than a year to unravel the chain of controlling computers and find out who was behind the GhostNet attack. In the end, the chain petered out in servers on Hainan Island off the coast of China, the home of one of the signals intelligence organizations of the People's Liberation Army." (ROSENZWEIG, 2013, pp. 28-29) e "A GhostNet, detetada em 2009, era uma rede de ciberespionagem de mais de de 1000 computadores comprometidos em 103 países tendo como alvos a informação política, diplomática , económica e militar." (CALDAS & FREIRE, 2013, p. 3)

127 "FOR OVER TWO DECADES, CYBERDEFENDERS have struggled to determine the source of the most damaging cyberattacks. This attribution problem will only become more critical as we move into a new era of cyberconflict with even more attacks ignored, encouraged, supported, or conducted by national governments. Analysts often fall into the trap of 'attribution fixation,' believing that attribution must start at the lowest, most technical levels. Only once these technical forensics of determinating the identity of attacking and controlling machines are established, as the thinking goes, can attribution hope to determine the person or organization responsible. This process rarely succeeds but fortunately, as this paper will show, there is another option. […] ." (HEALEY, 2011, p. 57)

128 "This is a deeply disorientating phenomenon. We're used to a world in which a sovereign nation can control its own border traffic, bat that's almost impossible on the Internet. This lack of control is threatening to the entire structure of the international community. Since the Peace of Westphalia in 1648, sovereign nations have been defined by their ability to control territory and the transit of people and goods across that territory. Now, ideas and information flow across boundaries almost without limit, disrupting settled expectations and threatening the status quo." (ROSENZWEIG, 2013, p. 23)

129 "The uniformity of 1s and 0s in the logic layer of the Internet is what makes the magic of cyberspace information transmission possible, but all the 1s and 0s look the same. Different types of activities in the logic layer are difficult to distinguish. We can't tell what any given piece of computer code will do just by looking at it. The code that does ham in a piece of malware is called the payload. This is the executable portion of the program that tells an intrusion what to do. Once inside the computer, a program can steal, change, or destroy data; order a computer to send out spam; or, as we saw with Stuxnet, cause physical damage to a system it controls. But it's virtually impossible to tell in advance whether a particular piece

Virtualização e análise estatística inteligente dos *streams* de bits, poderá permitir, a médio prazo, comparar e descobrir padrões de sequências idênticas a outras, anteriormente identificadas, por isso semelhantes em comportamento malicioso ou portadores de vírus[DT&T03], *worms*[DT&T02], *Trojans*[DT&T08] (ver Anexo A.ii), etc.

O Cibercrime como "o asa" das Infraestruturas Críticas

> "In a classification of contemporary crises challenging the EU, cybercrime is defined as a transboudary crisis (Boin, Rhinard, 2008)*. Such classification comprehends external crises, namely threats beyond the EU borders; internal crises, i.e. contingencies within the EU boundaries; and transboundary crises, namely crises whose effects easily cross the geographical borders of the states. As a matter of fact, contemporary crises are changing in complexity and interconnection due to globalization and the consequent increase of mass communication and social fragmentation. As a result, traditional states' responses are not effective and self-sufficient tools of action." (NOTO, 2013, p. 6) *"*Managing Transboundary Crises: What Role for the European Union?"*, International Studies Review, Vol. 10, Issue 1, March 2008

A preocupação com o crescimento da *eSociety* em geral, e com o crescimento económico em particular na UE, e as respetivas implicações de segurança[130], fizeram com que a CE através da *DG HOME* e da *DG JUSTICE* procurasse aplicar as «linhas de atuação» presentes na referida Convenção de Budapeste de 2001 que entrou em vigor em 2004 e que constituiu, como já vimos, um «catalisador»[131] para a UE. Até ao ano passado, no entanto, só 36 dos 47 membros do *CdE* tinham procedido à sua ratificação iniciada em 2004. Dados consultados no sítio *web* do CdE a 25 de agosto de 2014 em http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG). Entre, os que não o fizeram, um deles tem vindo a ter uma visibilidade, substancialmente, negativa: a Federação Russa. Tendo, o Cibercrime tomado com o crescimento "exponencial" da Internet –«em 2000 cerca de 361 milhões de pessoas tinham acesso à Internet. Em pouco mais de uma década, o número de utilizadores de Internet cresceu 566,4%. Em 2012, mais de 2400 milhões de pessoas utilizavam a Internet.» (NOTO,

---

of code is an innocent e-mail communication or a full-scale cyber attack. Particular pieces of malware have unique signatures that allow us to distinguish them from innocent Internet traffic, but we usually come to recognize them only after the first attack has occurred. Thus, the initial attack will almost always get through. The only alternative is to treat all Internet traffic as malicious, and that's too difficult and intrusive to carry out." (ROSENZWEIG, 2013, p. 24)

[130] "It is worth noting that the EU fights cybercrime for security matters as well as economic ones. In fact, as even the Commission recognized, internet gives several opportunities to increase economic productivity. Consequently, combating cybercrime is needed to preserve the EU power of economic growth." (NOTO, 2013, p. 6)

[131] "The CoE Convention was like the catalyst of the European Union process for building her own instruments and norms of cybercrime fighting." (NOTO, 2013, p. 5)

2013, p. 2)–, proporções muito preocupantes e lesivas para a economia, comércio e para os cidadãos da UE –«Cerca de 368 milhões deles [utilizadores de Internet] vivem na UE, representando mais de 15% do total da população.» (NOTO, 2013, p. 2)– Na utilização indevida e fraudulenta de meios eletrónicos e de telecomunicações pelo Crime-organizado, endossaram as preocupações nas instituições, nos legisladores e gestores políticos ao nível de topo das instituições da União. A '***Ação 30–Estabelecer uma Plataforma de Cibercrime Europeia*'** e a **'*Ação 31–Análise da utilidade na criação de um Centro Europeu para o Cibercrime*'**, também, estão relacionadas e servem de apoio funcional à '***Ação–32 Robustecer a luta contra o cibercrime e ciberataques no plano Internacional*'** e à '***Ação 36–Suporte ao reporte de conteúdo ilegal*'** que, por sua vez, estão relacionadas com a '***Ação 125–Expandir uma Aliança Global contra o Abuso Sexual de Crianças on-line'*** –que já não pertence de forma direta, ao âmbito deste trabalho– e ao Pilar III da Confiança e da Segurança. A CE, o *DG HOME* e o *DG INTERNAL SECURITY* encomendaram, a seu tempo, um estudo de assessoria à *RAND*[132] *Europe* –cujo primeiro autor e responsável pelo estudo foi Neil ROBINSON–, intitulado ***´Feasibility study for a European Cybercrime Centre´***, fazendo parte do contrato HOME/2010/ISEC/FC/059-A2[LRG111] de fevereiro de 2012, que poderá ser obtido em http://www.rand.org/pubs/technical_reports/TR1218.html, consultado a 10 de fevereiro de 2014. Esse estudo foi orientado no sentido de saber se seria, mesmo, necessária a criação de um Centro Europeu para o Cibercrime. O trabalho contemplou a «criação de uma lista de possibilidade em que foram aplicados princípios de orientação baseados num pequeno grupo de opções, de maneira a que a mesma fosse razoável, mas deixando 'espaço de manobra' suficiente para permitir aos atores subsequentes do estudo a consideração de caminhos diferentes e alternativos de resolução do problema, baseado num leque de possíveis tipos de intervenção». Foi tida em consideração que, se a conclusão fosse pela criação de um Centro: "Como seria a sua implementação? Se como uma unidade autónoma ou dependente de que outra entidade já existente." O estudo preconizou vários cenários[133], tendo sido escolhido um cenário de compromisso:

[132] "A nonprofit, nonpartisan, and committed to the public interest research organization."

[133] "6.4 Craft option 0: Maintain the status quo This opinion involves improvements of current activities of the stakeholders identified in the research so far. […] For example, in this option we would envisage measures to strengthen the use of the intelligence databases by Member States, identify ways in which the combined voice of the heads of national HTCUs [High Technological Cyber Unit] could be heard (e.g. Through the EUCTF –[Financial Action Task Force]) and further strengthen existing activities and capabilities (e.g. with respect to training provision); 6.5 Draft option 1: An ECC owned by Europol This

«A criação de um novo Centro, mas ficando na dependência de uma instituição já existente e com experiência na área do crime transnacional europeu (e mundial, em cooperação com a *INTERPOL*[134]), a *EUROPOL*[135]» –Opção 1 «6.5 Do estudo: Um Centro Europeu para o Cibercrime sedeado junto da Europol[136]**»**–, que passou a estar sedeado em Haia, na Holanda. Este centro passou a designar-se como Centro Europeu de Luta contra o Cibercrime ou *European Ciber Crime Center–E3C* ou *EC*^{3}, e entrou em funcionamento no início de 2013[137]. A afirmação deste novo *E3C* no quadro

---

option has a lot of favour and interest at present, given Europol's role and current remit, especially the operation nature of the organization. Provision of investigative support (forensics, support with other MLATs [Mutual Legal Assistant Treaty] and Joint Investigation Teams) would be of an operational or collaborative nature given Europol's current mobile forensic capabilities, network and also links to Eurojust. Achieving the objective of intelligence-sharing would also be of an operational nature since Europol already has a well established intelligence apparatus in the form of the AWFs (albeit with room for improvements). With regards to outreach, this would be envisaged as collaborative in nature given the current legal framework as to what can and cannot be shared with the private sector). The role of Europol in being a point of strategic advice would necessarily be advisory in nature (as this would involve collecting and collating the views of different Heads of HTCUs across Europe). Similarly, contact development would be achieved in a collaborative way at Europol, via sharing information and working alongside the national HTCUs and other partners (e.g. industry). Running an internal 'one-stop shop' hotline could be an operational activity (in the same way as the current intelligence databases). Finally, if Europol were to try to achieve the objective of training then it would have to be a collaborative exercise, working alongside other training partners (such as CEPOL, ECTEG, academia and industry), noting that Europol also provides some training (e.g. in investigative techniques). **6**.6. Draft option 2: An ECC owned by Eurojust As the other operational agency, many of these aspects described above with respect to Europol are also relevant to Eurojust. However, providing intelligence functions would have to be collaborative since Eurojust would need to either rely on intelligence capabilities of Mamber States or of others such Europol. […]; 6.7. Draft option 3: An ECC owned by ENISA As the only 'core' EU-level stakeholder with a non-operational function, achieving many of the objectives indentified from the empirical evidence base would take the form of collaborative or advisory type of activity rather than direct operational intervention. ENISA has neither operational responsibilities nor mandate in the field of cybercrime. […]" (RAND Europe, 2012)

[134] "[…] Leading this effort in INTERPOL, which is planning to establish a central research and intelligence unit to combat cyber-crime, the Global Complex for Innovation (IGCI)*. Scheduled to be based in Singapore and training facilities and advanced computer forensics laboratories. In addition to evaluating and developing open source software for law enforcement authorities, the IGCI will provide assitence to states currently lacking sufficient cyber crime-fighting capabilities. * http://.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Inovation (accessed 23/Feb./2012)." (BENDIEK & PORTER, European Cyber Security within a Global Multistakeholder Structure, 2013, p. 169)

[135] "In 1999 also EUROPOL started its work*. The EU law enforcement agency deals with criminal intelligence exchanges and is active in combating cybercrime in cooperation with EUROJUST. *.EUROPOL was set through the Council Act of 26 July 1995 drawing up the Convention on the establishment of a European Police Office. However, EUROPOL Convention came into force on the 1st of October 1998 and the agency started its full activities on the 1st July 1999." (NOTO, 2013, p. 8)

[136] "7.12 Conclusion - Our recommendation based on the above assessment is that the most feasible option, given the mandate and the tasks that an ECC must undertake is for the ECC to be owned by Europol." (RAND Europe, 2012)

[137] "The European Cybercrime Centre (EC3) at Europol in The Hague was opened on 11 January 2013. EC3 aims to become the focal point in the EU's fight against cybercrime, through building operational and analytical capacity for investigations and cooperation with international partners. Leading ICT journalist, Jennifer BAKER, met with Troels OERTING, Head of European Cybercrime Centre**,** to

Europeu –integrado na *EUROPOL* e apoiado por outras agências, como é o caso da *ENISA* e do *EUROJUST*[138]–é essencial para o melhoramento do índice de confiança dos cidadãos nos mecanismos de segurança existentes e em funcionamento no Ciberespaço. Permite a persecução de ações ilegais perpetradas *on-line*, equivalentes àquelas levadas a cabo no mundo real das atividades económicas, financeiras, sociais e políticas da nossa sociedade europeia no quadro irreversível da globalização dos mercados financeiros, de produtos e de serviços.

No entanto, para um combate eficiente e sistémico ao Cibercrime, a UE tem de trabalhar em três planos distintos[139]: o primeiro, interno, de cooperação entre as instituições da União e os EMs, procurando esbater as sobreposições e catalisando as competências de cada um em prol da segurança dos cidadãos, das instituições e da manutenção do estado de direito; o segundo, a nível dos fóruns internacionais, mas de todos eles, mesmo aqueles que à partida possam não parecer relevantes de momento, uma vez que a natureza do cibercrime é transnacional e de origens variadas, através de uma cooperação sistémica na prevenção, na formação e na prossecução "dentro da Lei" em países terceiros, utilizando para isso, também, o SEAE[140] e a PESC; o terceiro, e talvez o mais importante, será potenciar os dois anteriores, criando sinergias comuns, servindo "o modelo" para uma extrapolação rumo a outras regiões, no futuro, não esquecendo os Valores Fundamentais da UE, i.e. proporcionar uma luta justa e rápida ao

discuss cyber security and EC3′s work." Consultado em http://www.vieuws.eu/citizens-consumers/1st-eu-cybercop-european-cybercrime-centre-focus-criminal-gangs/ a 30/mar./2014.

[138] "The Tampere European Council [15th and 16th of October of 1999] is important also for laying the basis for the creation of EUROJUST, the EU judicial cooperation agency*. EUROJUST was established through the Council Decision of the 28th of February 2002** and the fight against computer crime was mentioned within the agency mandate***. *Tampere European Council, Presidency Conclusions, conclusion 46. **Council Decision 2002/187/JHA *** Council Decision 2002/187/JHA, art. 4.1b." (NOTO, 2013, pp. 7-8)

[139] "Concerning, the fight against cybercrime, it is essential improving security standards and policies at the international level due to intrinsic transactional nature of this phenomenon. For this reason, the EU has to press forward further developments in the international cooperation against cybercrime also by involving other stakeholders and their expertise. All actors involved have face the challenge to handle this field in a more transparent and accountable way. Everyone must do its part. Given that not all actors involved can prioritize cybersecurity in the same way, it is good to let all the stakeholders be more involved in this field. (NOTO, 2013, p. 11)

[140] "Maybe, we should start to asking the countries that are stealing really at the beginning of these technologically development what exactly they should become, to help them and how to make them more resilient already from the outcome set, because they should not repeat our mistakes that we put all the system up than restart security with them maybe is possible for them have a little more resilient elements already in before they develop those systems." (TIIRMAA-KLAAR, 2013)

cibercrime, não conduzindo à sua "securitização"[141][208]em demasia, procurando, sempre, respeitar os Direitos Fundamentais dos Cidadãos dos EMs, assim como, os direitos legais na União dos perpetradores de atos de cibercrime até, durante e após o processo de acusação, julgamento e, se possível –pelo «problema da atribuição»–, condenação.

1.3 Estratégias de Segurança do Ciberespaço dos Estados-membros

As Políticas de Cibersegurança: Implementação a várias "velocidades"

A escolha de alguns EMs da União, em detrimento de outros, para servirem de exemplos através de documentos de estratégia para o Ciberespaço, reflete uma realidade incontornável. Tem com primeiro propósito indicar a pluralidade de pontos de vista – também nas políticas de Cibersegurança– aliás, normal e de salutar quanto baste/q.b., na UE[142]. Numa primeira análise, o que poderia denotar uma fraqueza, deveria ser, antes, uma vantagem, pelas realidades variadas e diferentes estádios de desenvolvimento tecnológico e económico-social, podendo levar à elaboração de uma estratégia, comum da UE, mais redundante e detalhada. Logo, necessariamente mais complexa na conceção, mas mais efetiva, funcional e menos sobreposta, evitando erros cometidos, anteriormente, por outros. O que pensamos não ter sido o caso, devido às múltiplas reações, não totalmente favoráveis em relação à UE-ECS, como já vimos e tornada pública a 07 de fevereiro de 2013. Como segundo propósito, pretende demonstrar a cada

[141] "This does not mean that the EU does not care about freedom, but preserving the citizen security is priority to preserving fundamental human rights". (NOTO, 2013, p. 7)

[142] "So when we come to a more policy response what we have seen so far, than I think the EU provides a very interesting example of different very resilient national governmental cyber models. Because seen at least three or four different models now emerging inside of the EU by the different regions and the different countries there and in then every nation in the role test to find their own model to become more defended, more resilient in this space. What we have in the EU right now, we can observe the Nordic strong voluntary Public-Private Partnership cooperation model, which also is possible in hands by the cultural institutional and organizational traditions of the Nordic nations, which I think Estonia belongs to, because we had a almost one thousand years of a certain culture of holding the society together, and that has help us to defend in ourselves also in cyber area. Then we have a more intelligence lead gentlemen agreement model, which is the UK-model. Where certain entities have good cooperation, coordination and agreements already that's back times it as already coordination takes back to the cold War times, were Critical Infrastructure (CI) is important and now this has been extended to cyber issues. Then we have a third model which is more top-down, regulatory model. This more deregister model possibly is thus continental-European or central-European or that some people says – French model. But I do not think we should associate this to one country, so, that is good see, there fills that we should regulate. That we should tell to the private sector what to do, or how exactly to do it. So, this kind of tendency is to see as well. So, as you know that EU proposal for a cyber directive still in the EU right now, and there policy makers are still deciding what kind of model and how, were and when this EU legislation will come out." (TIIRMAA-KLAAR, 2013, pp. 1-4':29")

vez maior "presença" dos EMs mais expressivos em dimensão e tecnologia –dir-se-ia com "velocidades" mais acentuadas, em detrimento dos outros, em «velocidades secundárias»[143]–no domínio das TICs, segurança interna, ação externa e assuntos relacionados. O seu respetivo "peso" interno, em Bruxelas na formulação das respetivas políticas, é cada vez mais assimétrico. O externo –por vezes autónomo e/ou descoordenado– ao nível global das Relações Internacionais no domínio da Ação Externa, realça-se de forma negativa, a cada iniciativa ou intervenção. Ambas as situações são contraproducentes, em relação a uma União que se pretende, mais participada, interativa e multilateral para um reforço da cidadania europeia, nos fóruns internos da "Comunidade"[144]. Também, mais interventiva e menos onerosa, porque partilhada e colaborante, ao nível estratégico e global, nomeadamente dos G7/G8 (Grupo de Países com Economias mais Industrializadas, na conjuntura atual, sem a FR), e não na forma retalhada, do cada um *per se*.

Estratégias de Cibersegurança: Pragmatismo e funcionalidade ou obrigação?

O valor global das várias estratégias nacionais dos EMs é, assim, menor –quanto mais não seja pela ausência de distância e de fronteiras no Ciberespaço[145], pela velocidade vertiginosa e propagação dos malefícios dos atores e das ações– do que se, as mesmas, tivessem sido tidas em conta devida na formulação da ECS apesar do excessivo tempo que demorou a construir[146]. Mas, não foi essa a mensagem que passou, nomeadamente no PE, apesar da veiculação de opiniões de funcionários com elevadas responsabilidades –na manutenção do *status quo*– e do esforço concertado das, três,

[143] "[…] to having different speeds, we already have it in the EU […] we have some Member states who/ that has gone beyond on certain level and others remaining behind." The European Policy Centre's leading EU politics expert Janis A. EMMANOULIDIS. Consultado em http://www.vieuws.eu/eu-institutions/post-eu-summit-takeaways-juncker-in-driver-seat-of-a-multi-speed-europe/ a 04/jul./2014 em 4':51".

[144] "EU Community-Building: Past and Future – The EU has sought to engage in community-building by building bonds of affinity among its citizens and by promoting shared values, not by introducing more top-down institutions." (ETZONI, 2011, p. 240)

[145] "Sovereignty, while referring to recognition and application of state authority, is a nuanced term, and differences in state application of authority provide a critical window of analysis. Westephalian sovereignty (derived from the Peace of Westphalia) is commonly the definition used when describing the implications of 'cyberborders,' […] KRASNER's 'domestic sovereignty' is perhaps a more apt term to describe structures of state authority*. * KRASNER, Stephen D., '*Sovereignty: Organized Hypocrisy'*, (Pinceton, New Jersey: Prince Princeton University Press, 1999)." (LOSEY, 2014, p. 86)

[146] "Let's talk about Cyber Security. The Cyber Security has been a long time 'in the making', the announcement has been delayed and so forth, […]" Leading ICT journalist, Jennifer BAKER a 07/fev./2013 em http://www.vieuws.eu/ict/eu-cyber-security-mep-in-t-veld-laments-lack-clear-strategy/ Acedido em 08/out./2013.

senhoras Comissárias nos *media*, através de *Marketing* político, etc.). No entanto, a sua existência real é, por si só, uma "vitória" para a CE e, talvez, para a União. Não deixa de ser uma, primeira "base de trabalho", necessariamente, a precisar de aperfeiçoamento e adaptação continuada ; porque «uma estratégia de (ciber)segurança não é um fim em si mesma, mas sim um processo retroalimentado com os erros, então detetados, e com as respetivas alterações da realidade ou da sua perceção[147]». Quanto à profusão de estratégias, entretanto, apresentadas, parece tratar-se de uma "obrigação", que cada EM tenha de formular e apresentar uma estratégia. Aliás, como, qualquer empresa ou organização mundial que queira ser tida em devida conta, como um "verdadeiro" ator ao nível do Ciberespaço. Com toda a certeza que há "estratégias" e Estratégias! As ultimamente concebidas na UE não têm sido, de forma cabal –ao nível da Academia e de alguns *think-tanks*, consideradas como tais, na segunda aceção. Há, as que foram pensadas para serem, mesmo, implementadas e obrigatoriamente funcionais, por necessidade imperiosa do País ou organização devido à sua vulnerabilidade ou interesse estratégico. De igual forma, há aquelas que foram decalcadas de outras, sem a necessária adaptação à realidade do País ou organização, porque era[/é] necessário publicar e apresentar formalmente uma estratégia, quanto mais não seja, para dissimular "que se tem uma estratégia." Como se isso, por si só, fosse dissuasor, o suficiente, para as vulnerabilidades existentes, desaparecessem –fruto da ausência de políticas coerentes e sistemáticas, insuficiência de recursos humanos com formação adequada–, meios materiais e financeiros, falta de uma "cultura de segurança" ao nível do cidadão como utilizador da Internet, do trabalhador ou das organizações público-privadas, etc.

Os documentos publicados na Internet apresentam, invariavelmente, uma "justificação" da razão de ser do mesmo, um cenário de contextualização em que o documento "faça sentido", uma panóplia de perigos reais e outros extrapolados –não chegando ao exagero americano[34]–, referindo pelo menos uma organização, ou grupo, de implementação ou coordenação do que é registado no documento e procedimentos "genéricos" a efetuar nos tempos próximos. Compreende-se que por razões relacionadas com a confidencialidade dos temas, não seja descrito para além do, estritamente essencial. São ignoradas também questões de natureza técnico-operacionais ou

[147] "The information technologies used are subject to short innovation cycles. This means that the technical and social aspects of cyberspace will continue to change and bear not only new opportunities, but also new risks." (Federal Ministry of the Interior, 2011, p. 13)

orçamentais de implementação da ações descritas nos mesmos –podendo sê-los como complemento, noutros documentos mais técnicos e/ou reservados, como é o caso da Holanda, https://www.ncsc.nl/english/current-topics/news/cyber-security-assesment-netherlands.html ou https://www.ncsc.nl/english/current-topics/news/best-practices-in-computer-network-defense.html consultados em 13 de junho de 2014– , mas ignorando os pontos nucleares de uma "verdadeira" Estratégia[148], plena e funcional.

A Estratégia do Reino Unido: Proteção e Promoção no Mundo Digital

> "Citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space: working together, at home and overseas, to understand an address the risks, to reduce the benefits to criminals and terrorists, and to seize opportunities in cyber space to enhance the UK's overall security and resilience." (Citando a Estratégia de Cibersegurança do UK, 2009, p.3)

O Reino-Unido, devido à sua condição de relativo grau de industrialização, no contexto global, em particular na produção de energia nuclear, e de afinidades –linguísticas e culturais– com os EUA, foi co pioneiro no que diz respeito às preocupações com a segurança do Ciberespaço, mormente, em relação às vulnerabilidades das PICs, com maioria de razão, após o 11 de setembro e o ataque terrorista em Londres (2005) e as possíveis consequências reativas (por parte dos islamitas radicais) da participação do País, unilateralmente –com os EUA– no sul do Iraque, em Bassorá, quer ainda, ao nível da ONU e da OTAN no Afeganistão. Acrescido a estes fatores, a consequente migração de serviços, nomeadamente, financeiros, e de largos setores de comercialização e distribuição de produtos[30] e outros serviços para a Internet, veio introduzir novas e complexas preocupações às empresas do setor privado e às organizações públicas e aos decisores políticos do País. Sendo assim, mesmo antes da apresentação da estratégica de Cibersegurança do Reino Unido, alguns dos tópicos já estavam implementados, ainda que de forma rudimentar, em ralação às PICs e aos serviços de proteção civil, à área de recolha de informações e a sua colaboração no *ECHELON* e com a *NSA*. No que concerne às PICIs, só muito recentemente, por exemplo e como atrás se disse, passou a estar plenamente funcional o

[148] "What is strategy? Strategy is a *tool* at the service of policy-making. Starting from the fundamental values of the policy-maker and the interests that are vital to upholding those values, strategy defines (1) the priority long-term objectives to be achieved, (2) the types of instruments to be applied to that end, and (3) the means to be allocated. The result is a long-term reference framework for short-term, day-to-day policy-making in a rapidly evolving and complex environment – a guide for strategic behavior.** Ctando BISCOP, Sven & COELMONT, Jo, *"Europe, Strategy and Armed Forces. The Making of a Distictive Power* (Abingdon: Routledge, 2012)" (BISCOP, 2012, p. 8)

CERT-UK, o que denota a complexidade de *Full Operational Capability–FOC* de um organismo que se pretende ao mesmo tempo, rápido, eficiente e abrangente, quer quanto à tecnologia empregue na deteção e resposta, quer ainda, quanto à amplitude de operacionalidade a todo o território de jurisdição que lhe é confinado pelos responsáveis legitimamente eleitos, neste caso particular de forma direta, uma vez que este *CERT* depende do *Minister for the Cabinet* Office/Vice-Primeiro Ministro, Francis MAUDE.

Do documento, é relevante, a primeira das ambições definidas dos quatro macro objetivos a atingir, já em 2015, é imensamente complexa e difícil de alcançar: «1–O Reino Unido pretende 'placar' o cibercrime [tornando-o irrelevante] e vir a ser um dos mais seguros lugares do mundo de forma a facilitar os negócios no Ciberespaço;» As restantes são consideradas concomitantes com os desejos dos restantes países de expressão económico-política do *UK*: «2–O Reino Unido pretende ser mais resiliente a ciberataques e mais hábil na proteção dos seus interesses no Ciberespaço; 3–O Reino Unido tem colaborado na conceção de um Ciberespaço mais aberto, estável mas dinâmico no qual os cidadãos, empresas e organizações do País possam sentir-se seguras e com isso suportar [outras] sociedades abertas; e, 4–O Reino Unido pretende deter um conhecimento incisivo e transversal, competências e capacidades suficientemente adquiridas para levar a cabo todos nos seus objetivos relacionados com a Cibersegurança.» (Citando a Estratégia de Cibersegurança do *UK*, 2009, p.9)

Tendo em conta o objetivo da segunda parte deste trabalho convém abordar, ainda que com a limitações de acesso a dados disponíveis, ficando pelos disponíveis, não confidenciais e relativos a 2012, descrever as capacidades descritas no *Military Balance* que respeitam ao Reino-Unido:

> "The Office of Cyber Security & Information Assurance works with the Cyber Security Operations Centre and ministries and agencies to implement cyber-security programmes. CSOC [Cyber Security Operations Centre] is hosted by GCHQ and was also established in 2009. The UK´s October 2010 Strategic Defence and Security Review said that the country would 'establish a transformative national programme to protect ourselves in cyber space'. This 'National Cyber Security Programme' is supported by some £650m - with programme management by OSCIA - and led to a new Cyber Security Strategy, published in November 2011. A UK Defence Cyber Operations Group was set up in 2011 to place 'cyber at the heart of defence operations, doctrine and training'. This group was transferred to Joint Forces Command on this formation´s
> establishment in April 2012." (Military-Balance Online, 2013, p. 103)

Por este trecho podemos inferir uma coordenação interna entre autoridade civis e militares, potenciando cada uma delas no seu meio e aproveitando-as para o objetivo último e comum ao serviço das instituições e das organizações que fazem funcionar a economia e produtividade do País. Seria bom, que ao nível da União, soubessem os EMs aproveitar a pertença, também à OTAN –ou sua parceria– no sentido de não desperdiçar recursos, escassos, e de potenciar conhecimentos e técnicas já apreendidas e testadas para seu próprio benefício e da União em ações internas ou de ação externa.

A Estratégia da Alemanha: Simplicidade, pragmatismo e eficácia

> "The availability of cyberspace and the integrity, authenticity and confidentiality of data in cyberspace have become vital questions on the 21st century. Ensuring cyber security has thus turned into a central challenge for the state, business and society both at national and international level." (European Network and Information Security Agency ENISA, 2012, p. 4) citando a Estratégia Alemã para a Cibersegurança (Federal Ministry of the Interior, 2011, p. 2)

A República Federal da Alemanha como portento industrial mundial, (na aeronáutica e espaço –o atual Diretor Executivo da *ENISA*, Doutor Udo HELMBRECHT, foi, antes, diretor de segurança de TICs na maior empresa aeronáutica e do espaço da Alemanha, a ***MBB-ERNO Raumfahrttecnik GmbH***–, no automóvel, na naval e no ferroviário, na saúde –diagnóstico/tratamento–, farmacêutica, química e agroalimentar, produção e controlo industrial –com as suas massivas incorporações de eletrónica, informática e comunicações), esteve na linha da frente, quanto à necessidade, de acautelar as PICs[149]. Também de forma transversal, com as PICIs ligadas à produção de *software*, fornecimento de serviços financeiros, de seguros, e complementares, levaram os decisores políticos e os responsáveis técnicos das agências federais, a ter o cuidado de ir implementando ações preventivas no domínio da segurança do "seu" Ciberespaço[150] e na Internet. Sempre que tiveram a Presidência da União procuraram –ou assessorar outros EMs de adesão mais recente da sua esfera de influência, República Checa, Letónia, Lituânia, EE, etc.–, na condução deste tipo de matérias induzindo-os

[149] "At federal level, the following areas have been identified: Energy; Information technology and telecommunication; Transport; Health; Water, Food; Finance and insurance sector; State and administration; [and], Media and culture." (Federal Ministry of the Interior, 2011, p. 15)

[150] "[…] For example, in response to US international surveillance, German Chancellor MERKEL proposed a German internet with Deutsche Telekom routing traffic to stay within the Schengen area*. ** HILL, Jonah Force, '*The Growth of Data Localization Post-Snowden: Analysis and Recommendations for US Policymakers and Business Leaders.*' Conference on the Future of Cyber Governance, The Hague Institute for Global Justice (2014)" (LOSEY, 2014, p. 86)

nas agendas dessas presidências para o "bem comum(nitário)". Note-se, ainda, que a brochura de ECS da Alemanha é pragmática e sucinta, aliás como apanágio da forma de pensar e agir germânica. De seguida, mostra-se um diagrama simplificando as articulações da política de Cibersegurança da Alemanha:

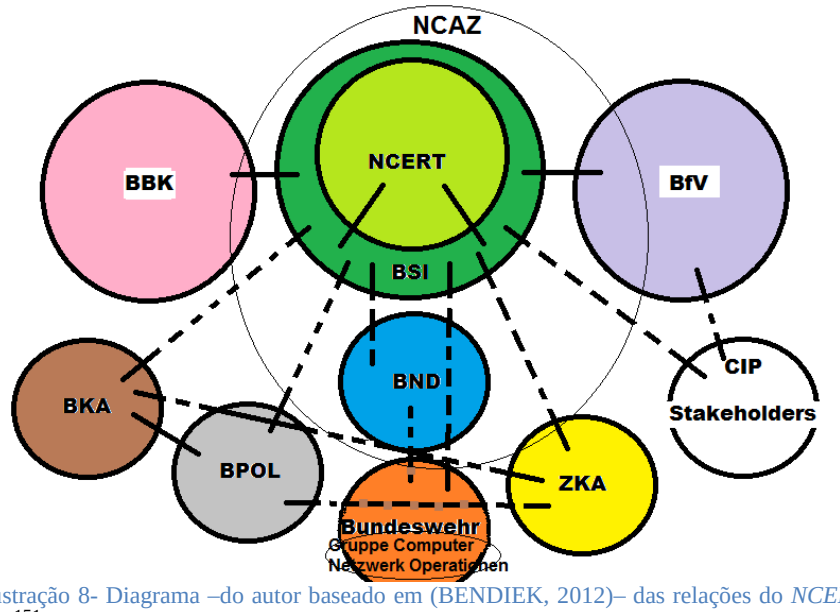

Ilustração 8- Diagrama –do autor baseado em (BENDIEK, 2012)– das relações do *NCERT-DE*.[151]

Fontes Estratégia de Cibersegurança da Alemanha (Cyber Sicherheitsstrategie für Deutschland), (BENDIEK, "European Cyber Security Policy", 2012, p. 13) e (BENDIEK & PORTER, European Cyber Security within a Global Multistakeholder Structure, 2013, pp. 165-166)**, Legenda das siglas significativas:** *BSI* **–** ***Bundesamt für Sicherheit in der Informationstechnik*** – Federal Office for Information Security**,** *BND* **–** ***Bundesnachrichtendienst - Federal Intelligence Service,*** *BfV* **–** ***Bundesamt für Verfassungsschutz*** **–** Serviço de Segurança Interna e Contraespionagem**,** *BBK* **–** ***Bundesamt für Bevölkerungsschutz*** - Federal Office of Civil Protection and Disaster Assistance**,** *ZKA* **–** ***Zollkriminalant*** **-** Customs Criminological Office**,** *NCAZ* **–** ***Nationales Cyber-Abwerzentrum*** – National Cyber Defense Center *e GCNO* **–** ***CNO+Strategy Reconnaissance***

No que concerne aos recursos ligados de forma direta às forças armadas, mas que têm relações privilegiadas com outras organizações ao nível governamental-federal será conveniente verificar a situação da Alemanha nesse aspeto particular:

[151] "4. National Cyber Response Centre – The operational cooperation between all state authorities and improve the coordination of protection and response measures for IT incidents we will set up a National Cyber Response Centre. It will report to the Federal Office for Information Security (BSI) and cooperate directly with the Federal Office for the Protection of the Constitution (BfV) [Serviço de Segurança Interna e Contraespionagem] and the Federal Office of Civil Protection and Disaster Assistance (BKK). Cooperation in the National Cyber Response Center will strictly observe the statutory tasks and powers of all authorities involved on the basis of cooperation agreements. The Federal Criminal Police Office (BKA), The Federal Police (BPOL), the Customs Criminological Office (ZKA), the Federal Intelligence Service (BND) [Serviço Federal de Informações e Espionagem], the Bundeswher and authorities supervising critical infrastructure operators all participate in this centre within the framework of their statutory tasks and powers." (Federal Ministry of the Interior, 2011, p. 8)

> "Germany established a Department of Information and Computer Network Operations in 2009 under the guidance of the then-chief of the Bundeswehr's Strategic Reconnaissance Command. Bundeswehr units maintain organic IT monitoring capability: a Bundeswehr CERT team (CERTBw) is available. Germany issued a Cyber Security Strategy in February 2011. A National Cyber Response Centre, involving police, customs, the Federal Intelligence Service and the Bundeswehr, began operations on 1 April 2011. It reports to the Federal Office for Information Security. A National Cyber Security Council has also been established, with high-level representatives from government and, as associate members, businesses." (Military-Balance Online, 2013, p. 52)

Parece-nos que, aqui também e, à semelhança do Reino-Unido, tem havido o cuidado de uma implementação que tente obter "mais do que a soma das partes" com responsabilidades no domínio do Ciberespaço. No entanto o documento é menos extenso e mais objetivo do que o do Reino-Unido, logo, menos narrativo e disperso. O que é recomendável para o público a que se destina, incluindo o cidadão comum, desperto para este tipo de questões, porque utilizador das TIC e da Internet.

A Estratégia da França : Reconquistar o estatuto "Gaulista" no Ciberespaço?

> "Le cyberspace, nouvelles Thermopyles, est devenue un lieu d'affrontement: appropriation de donnés personnelles, espionnage du patrimoine scientifique, économique et commercial d'entreprises victimes de leurs concurrents ou de puissances étrangères, arrêt de services nécessaires au bon fonctionnement de l'économie ou de la vie quotidienne, compromission d'informations de souveraineté et même, dans certaines circonstances, perte de vies humaines sont aujourd'hui les conséquences potentielles ou réelles de l'imbrication entre le numérique et l'activité humaine." (Agence Nationale de la Sécurité des Systèmes d'Information, 2011, p. 1)

A França, não tendo as especificidades externas do Reino-Unido –na sua relação com os EUA, i.e., a sua participação em locais de alto risco, com as exceções da intervenção na Líbia e, a mais recente mas não menos importante no Chade– tendo, igualmente, como a Alemanha uma comunidade de imigrantes, de segunda e terceira gerações, esta, de origem turca, assim como, o Reino-Unido de origens paquistanesa, de Bangladesh, etc., uma considerável população de origem muçulmana variada, –mormente magrebina–, tem de acautelar-se contra o "Mega terrorismo" islamita. Tendo, também, uma vital produção industrial de energia nuclear –no que se refere à percentagem de consumo interno–, e tendo muita produção industrial tecnológica na aeronáutica e espaço, no automóvel, na naval e no ferroviário, na saúde –diagnóstico/tratamento, farmacêutica e cosmética–, química e agroalimentar, produção e controlo industrial. Estas últimas, com as suas massivas incorporações de eletrónica, informática –como a produção de *software* livre– e comunicações, assim como, tendo

todo um passado de tradição quanto a uma certa autonomia científica e tecnológica, nomeadamente, no nuclear, aeronáutico e espacial militar, procurou de forma proactiva acautelar a segurança das PICs e da PICIs. Por fim, não devem ser esquecidos os mercados de serviços financeiros, de seguros e de turismo. Pelo que o lançamento da sua estratégia de Cibersegurança foi, uma consequência "natural" de necessidades já parcialmente pensadas e implementadas pelos responsáveis políticos e técnicos do País. Isso, também, é refletido no trecho do *Military Balance* de 2013 que passamos a transcrever :

> "The French Network and Information Security Agency (ANSSI), under the authority of the prime minister and attached to the office of the secretary-general for national security and defence, was established in 2009 to conduct surveillance on sensitive government networks and respond to cyber attacks. The 2008 French Defence White Paper placed emphasis on cyber threats, calling for programmes in offensive and defensive cyber-war capabilities. The White Paper noted that part of the offensive capability 'will come under the Joint Staff and the other part [⋯] developed within specialised services'. CALID (Analysis and Combat Centre for Computer Defence) monitors military networks and counters intrusions in coordination with ANSSI. In July 2011, the MoD produced a classified Joint Cyber Defence Concept. Ahead of the new Livre Blanc, the general secretariat on defence and national security (SGDSN) released a preparatory document stressing the strategic dimension of cyber threats and confirming the development of technical capabilities to control access to cyberspace. In addition, France is strengthening bilateral relations with strategic partners and through EU and NATO frameworks France has a national CERT, is involved in informal CERT communities, and is a member of the European government CERTs Group (ECG)" (Military-Balance Online, 2013, pp. 48-49)

As espectativas da França são ambiciosas e estratégicas, incluindo a vertente da Ciberdefesa: «1–Ser uma potência mundial na área da Ciberdefesa;» Isto, com a contribuição da sua própria indústria (como atrás já se referiu, com pergaminhos na área da defesa –nuclear, aeronáutica e espacial, naval– muito por visão estratégica e autónoma –em relação aos dois blocos da Guerra-Fria– do seu primeiro Presidente da V República, General Charles de GAULLE) Isto, de forma autónoma[152] e/ou integrada, de forma alargada, na AED, como consequência do Conselho de 19 e 20 de dezembro p.p. sobre estas questões; Quer ainda a França, como os restantes EMs de significância nesta

[152] "Tout en conservant son autonomie stratégique, la France doit effectuer l'effort nécessarire pour appartenir au premier cercle très restreint des nations majeures dans le domaine de la cyberdéfense. Nous bénéficierons ainsi de l'effet démultiplicateur des coopérations tant au plan opérationnel que pour la mise en place d'une stratégie unifiée face à des menaces communes." (Agence Nationale de la Sécurité des Systèmes d'Information, 2011, p. 7)

matéria: «2–Garantir a liberdade de decisão da França na proteção da Informação de Soberania; 3–Reforçar a Cibersegurança das infraestruturas críticas nacionais; e, 4–Assegurar a segurança no [seu] Ciberespaço.» (Agence Nationale de la Sécurité des Systèmes d'Information, 2011, pp. 11-14)

1.4 O papel dos Estados-membros de pequena dimensão

> "From the small state [caso da Finlândia e, também, presumivelmente no futuro, de Portugal][*] perspective, globalization has been particularly problematic. In general, power has been flowing away from all states to structural forces such as the financial markets, and from small states to big states. To counteract this loss of power, small states have traditionally concentrated their efforts on building multilateral institutuions and on participating in key international foruns where collective decisions are being taken. [*]'with a highly specialized economy, the multilateral frameworks for securing global flows are crucial.' In Abstract" (AALTOLA, SIPILÄ, & VUORISALO, 2011, p. 7)

> "Global and regional cooperation is an imperative; the only winning move is to play – with others." Idem p. 6

Numa primeira análise, não resta outra opção aos EMs de pequena dimensão em saber explorar os "nichos" de intervenção especializada, em campos de atuação muito específicos ou, conjunturalmente, favoráveis –de que detenham conhecimento ou competências pré-adquiridas e reconhecidas. Quer por via de "janelas" temporais extemporâneas ou criadas casuisticamente, quer ainda, por dispersão dos EMs de significância –que não as equacionaram com a oportunidade ou importância, devidas, nas referidas agendas nacionais ou institucionais internacionais. Ou, ainda, através de iniciativas multilaterais, conjuntamente, com outros parceiros de dimensão ou afinidades semelhantes[153], potenciando conhecimentos precocemente e implementando medidas concebidas e coordenadas em *pool* de cooperação. Podem intervir, também, através de propostas apresentadas nos fóruns em que são parceiros ou membros de pleno direito. Poderá ainda, nesta segunda hipótese, haver lugar para participação dos EMs de menor dimensão como "subatores" de estratégias definidas e consignadas a EMs de expressão significativa que, por razões operacionais ou de interesse conjuntural

[153] "Este projeto, que define as implicações e a perceção do impacto do ciberespaço na Segurança e Defesa dos Estados, pretende caracterizar o enquadramento concetual e operacional adotado por Portugal Espanha. Neste contexto, tendo em conta os esforços atualmente em curso nos dois países, procura-se identificar pontos de convergência e refletir sobre a possibilidade de desenvolvimento futuro de iniciativas conjuntas, sobretudo de natureza bilateral, mas também multilateral, no quadro das organizações internacionais, em particular da OTAN e da UE." (Instituto de Defesa Nacional, 2013, p. 5)

ou tático, possam delegar nos primeiros a sua realização e/ou monitorização. Pela perceção da situação atual na UE [em que o(s) diretórios prevalecem e o comunitarismo[154] diminui a cada dia que passa, estando cada um mais preocupado consigo e com os seus problemas nacionais, com a sua Opinião Pública e com os episódios de política doméstica a dominar as suas agendas], caberá a cada EM definir e preparar-se para a(s) estratégia(s) a seguir. Por fim, saber explorar, oportuna e cabalmente, as oportunidades que lhes possam surgir num cenário vertiginosamente dinâmico de economia globalizante, em geral, e altamente volátil e difícil de prever, como é o caso particular que nos ocupa neste trabalho, do Ciberespaço.

Estónia: De vítima (2007) ao pelotão da frente na Cibersegurança da UE

> "Estonia as an *'e-State´* - The significance of small states within multilateral fora is often underestimated and misunderstood because the focus is rather on power than on influence. In fact, small states have demonstrated that they are capable of acting strategically to preserve security while contributing to the stability and efficiency of international organizations[*]. In addition, smaller nations are more likely to launch initiatives that appear to be small contributions, but, in time, prove to be major developments[**]. Because these nations have a tendency to suffer from inferiority syndromes they are tempted to 'show their mettle' by trying to excel in their initiatives[***]. [*] MOSSER, Michael W., 'Engineering Influence: The Subtle Power of Small States in the CSCE/OSCE,' in REITER, Erich and GÄRTNER, Heinz, 'Small States and Alliances,' Physica-Verlag, New York, 2001, pp. 63-84. [**] DUKE, Simon W., 'Small States and European Security,' in REITER, Erich and GÄRTNER, Heinz, 'Small States and Alliances,' Physica-Verlag, New York, 2001, pp. 39-50 [***] SCHMIDL, Erwin A., 'Small Sattes and International Operations,' in REITER, Erich and GÄRTNER, Heinz, 'Small States and Alliances,' Physica-Verlag, New York, 2001, pp. 85-88" (LAASME, 2012, p. 9)

[154] "Indeed, studies show that movement toward building a European community has led to stronger alienation among millions of European citizens.[*] According to an analysis of Eurobarometer surveys from 1973-2004, net public support for the EU grew steadily in the 1980s (averaging about 42 percent) and reached an apex of 62 percent in 1991,[**] However, support then declined. By 1997, net support for integration had fallen to 39 percent. Since 2004, it has fluctuated within a 10 percentage point range to roughly 30-40 percent.[***] In 2010, net support was only 31 percent." .[*]For additional studies of patterns in public support for the EU not discussed here, see: Matthew GABEL, 'Public Support for European Integration: An Empirical Test of Five Theories,' *The Journal of Politics* 60, no. 2 (May 1998): 333-354; Liesbet HOOGHE and Gary MARKS, 'A Postfunctionalism Theory of European Integration: From Permissive Consensus to Constraining Dissensus,' *British Journal of Political Science* 39 (2009): 1-23. [**] The Eurobarometer is a bi-annual survey of public opinion by the European Commission. http://ec.europa.eu/public_opinion/index_en.htm; Net public support refers to the percentage of those who say their country´s membership in the EU is a good thing minus those who say it is a bad thing; Richard C. EICHENBERG and Russel J. DALTON, 'Post-Maastricht Blues: The Transformation of Citizens Support for European Integration, 1973-2004,' *Acta Politica* 42 (2007): 128-152, Figure 1. [***] European Commission: Public Opinion, *Eurobarometer Survey*, 2004-2010, http://ec.europa.eu/public_opinion/index_en.htm; " (ETZONI, 2011, p. 238)

A Estónia é um *case-study* paradigmático, chamado de «Inesperado Catalisador» do Ciberespaço Europeu e ocidental (LAASME, 2012, p. 9). O seu *CERT* foi criado em 2006, logo, antes dos ciberataques do ano que se seguiu, muito por força da estratégia do País em tornar-se um *e-State*, por razões que se prendiam com a situação conjuntural. Por um lado, consequência de República da ex-URSS, pobre em recursos e de pequena dimensão, e, por outro, de ter «escolhido» enveredar pela área das TICs como estratégica para o seu desenvolvimento, porque a globalização assim o aconselhava e, também, pelo exemplo da vizinha Finlândia, como caso de sucesso, recente, no setor.

No entanto, só por si, a existência do *CERT*, não foi suficiente[155] para que fosse a primeira vítima da história do Ciberespaço por parte de um ator estatal, ainda que através de *proxies* (os chamados *hackers* patrióticos, quem sabe, controlados de forma direta pelas forças de segurança do Estado da FR). Apesar de ter havido danos à economia e aos cidadãos, com a falha generalizada dos sistemas de administração pública e de privados que utilizavam a infraestrutura do setor de telecomunicações e Internet[156], durante alguns dias – num País com alta dependência das TICs –, aqueles não foram tão substanciais como se faria supor. Tudo isso «resultou contraproducente

[155] "[…] Because, we cannot really speak about the defence in traditional terms, when we speak about cyber issues. Cyber, is such, a very non-state concept, is IT technology in a way, innovation by the private sector and civil society enthusiasm, than asked to the Internet in last decades. So, this is a very anti-governmental concept. Governments are not easy to deal with this kind of asymmetric networking type of new entities because the Governments are more hierarchical, Governments rely on certain procedures and processes and Cyberspace is something new for the Governments. […]Then, also cyberspace is not hierarchical, cyberspace is a network. In order to have a good resilient structure, a good crisis management structure, a good defence strategy, we have to start thinking as a network, is network against network, is not network against hierarchy, because, and I am very sorry, but the hierarchy will be loose, and this is something that we have/has been learned in 2007 in Estonia. That was a network of non-state actors, that helped to defende of the attacks, it was not a government agency, it was not only one organization in the coutry, it was a network of different organizations that coordinate and that how we could resist of three weeks of serious DDoS attacks." (TIIRMAA-KLAAR, 2013)

[156] "[…] , which turned into an emotional outpour in the ciber domain by 27 Abril. From that day on the attacks became increasingly more sophisticated and coordinated and at their peak the internet traffic targeting Estonian government sites was almost 400 times above the normal raffic rate [tratava-se de uma ataque massivo do tipo DDoS (Distributed Denial of Service) recorrendo a uma rede expressiva de Botnets espanhados por mais de cem países] . Among other methods, the attackers utilized huge botnets for distributed denial of service (DDos) attacks, defaced the website of the Estonian Reform Party and sisrupt domain name service (DN) services in parts of the country[*]. To mitigate the consequences to national security, the Estonian information technology (ITC) managers had to block the international connections to the servers, which created a situation akin to a modern blockade of a country without concomitant deployement of any conventional weapons.[**] [*] KASK, Kadri, ENEKEN, Tikk and VIHUL, Liis, "Internatonal Cyber Incidents: Legal Considerations", NATO Cooperative Cyber Defence Centre of Excellence, Tallin, 2010, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf .[**] LAASME, Häly. "Estonia: Cyber Window into the Future of NATO", *Joint Force Quarterly*, issue 63, 4th Quarter, 2011, National Defence University, http://www.ndu.edu/press/estonia.html" (LAASME, 2012, p. 11)

para a estratégia de política externa da FR» –não produzindo os efeitos pretendidos, na altura. Provou mais uma vez que um «David pode 'derrotar' um Golias e deu o ímpeto que a Estónia necessitava para ser implementado o Centro, mesmo ali, ao lado, da fronteira Russa.» E, como lá diz o ditado : "há males, que vêm por bem!". E assim, foi devido àquele infortúnio que as ações subsequentes permitiram à Estónia ter passado de uma vítima do Ciberespaço para um exemplo a seguir, na implementação de uma completa política de Cibersegurança para o Ciberespaço, conseguido pela validação da sua estratégia inicial de ser membro da OTAN e da UE, apesar de ser um estado de expressão reduzida em ambas as organizações. Tendo sido sedeado na sua capital o *CCD CoE* [157] da OTAN para a Cibersegurança e Ciberdefesa –uma ambição datada de 2002 mas, sucessivamente, adiada pela OTAN– , e passando a contar, posteriormente, com a participação de alguns países da UE. O *CCD CoE* foi-se incrementando numa parceria muito estreita com a *ENISA* para assuntos de Cibersegurança relacionados com a UE. Em consequência de estar no "pelotão da frente" já reviu a sua Estratégia de Cibersegurança, sendo um parceiro OTAN/UE a ter em conta, no presente, e também amanhã, mesmo em termos relativos militares, como se pode constatar no relatório de 2012 do *Military Balance*.

> "Estonia established CERT-ee in 2006 and has further developed its cyber-security infrastructure after the cyber attacks of 2007. It adopted a national Cyber Security Strategy in 2008 [pelo Ministério da Defesa]. This strategy is due to be updated in 2013. In 2011, the Ministry of Economic Affairs and Communication was given overall responsibility for cyber security which it addresses through the Estonian Informatics Centre and the Department of State Information System. As well as domestic capacities, Tallinn hosts the NATO Cooperative Cyber Security Centre of Excellence, established in 2008 to enhance NATO's cyber-defence capability." (Military-Balance Online, 2013, p. 41)

A Holanda e o "contra relógio" do *Hub* da União Europeia

> "The Netherlands is the European leader in responding to technological trends and the effective use of ICT tools and Skills. The Netherlands is also an international hub, has the world's most competitive internet market and has one of the highest numbers of internet users. Safeguarding digital security and freedom and maintaining an open and innovative digital domain are preconditions for the proper functioning of our society. Therefore, we published the first National Cyber Security Strategy ($NCSS_1$) in 2011. The purpose of the $NCSS_1$ was to realize a secure, reliable and resilient digital domain

[157] "The CoEs [Center of Excellence e não Concil of Europe] are a supporting network of NATO by developing doctrines, improving interoperability, offering consultations, education and training, and collaborating in research and development. […] Currently, there are 18 accredited CoEs, plus 3 in development, one in almost every post-Soviet Eastern European country and without any doubt these are causing political headaches in the members of the Russian government." (LAASME, 2012, p. 17)

> through an integral cyber security approach based on public-private partnerships, as well as to seize the ensuing opportunities for society. […] In Order to be able to continue to respond to these threats, the Netherlands plans to further strengthen and extend their alliances with public and private parties, both national and international. This involves not viewing cyber security as an isolated element, but rather in correlation with human rights, internet freedom, privacy, social-economic benefits and innovation. The National Cyber Security Strategy 2 ($NCSS_2$) explains this broader government vision on cyber security and states responsibilities and concrete steps." Forward of National Cyber Security Strategy 2 from Netherlands, The Minister of Security and Justice OPSTELTEN, I. W.

Obtido em https://www.ncsc.nl/english/current-topics/news/new-cyber-security-strategy-strengthens-cooperation-between-government-and-businesses.html, consultado em 13 de junho de 2014.

Este excerto da introdução da segunda versão da ECS da *NL* (assim como já havíamos visto, da EE) reafirma algo já dito, de tornar o País como mais um *hub* do Ciberespaço –subentenda-se para a UE em relação ao mundo globalizado[158]. Poderemos induzir que os responsáveis do País engrenaram a problemática antevista para os próximos anos da *IG* na sua revista Ciber Estratégia com o intuito de ser a "Bússola" da Holanda entre 2014-2016 no domínio da cibersegurnaça. Achamos que, apesar de ser um EM de "pequena dimensão" na UE (devido à sua população e território relativos e ao "peso" que detém a nível político e de Produto Interno Bruto (PIB/*Growth Domestic Product–GDP*) conseguem, com os recursos que têm (apesar das restrições orçamentais), com inteligência e bom senso, utilizando os seus recursos humanos competentes e bem treinados, permitir-lhes ter acesso a uma Estratégia muito interessante, realista e pragmática.

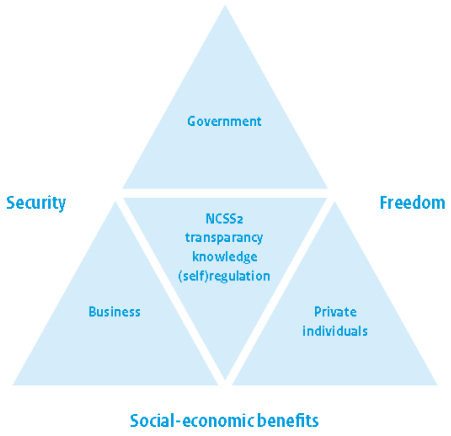

Ilustração 9- Relações tripartidas: Governo, Cidadãos e Empresas em CERT-NL.
Fonte (https://www.ncsc.nl/english) consultado a 04 de junho de 2014

[158] "The Netherlands wants to become the Digital Gateway to Europe." (2. Developments that call for action of National Cyber Security Strategy 1 from Netherlands)

A visão da segunda revisão da ECS holandesa revela um equilíbrio regulador inteligente, com conhecimento transparente e, cada vez mais, necessário entre os vetores Segurança e Liberdade aplicados, respetivamente, aos planos de atuação «Administração Pública–Negócios» e «Administração Pública–Cidadãos» prognosticando o cenário –de compromisso– a médio-prazo na *IG*.

Como membro da OTAN a Holanda tem, de igual modo, uma componente de Ciberdefesa e de Cibersegurança de forças militarizadas que têm relações de troca de informações e de procedimentos de atuação que pertencem ao foro confidencial. No entanto era esta a situação desses organismos até ao início de 2013.

> "In early 2011, the Dutch defence minister indicated that cyber defence would attract some of the Netherlands' declining budget and, beetween 2011–2015, around €30 million plus staff would be allocated, with full capability by 2016. In June 2012, the defence ministry launched a Defence Cyber Strategy to direct military cyber efforts. Among other elements, the strategy is intended to strengthen cyber defence, and 'develop the military capability to conduct cyber operations (offensive element)'. In developing these, the document says that 'optimal use will be made of the expertise and assets of the Defence Intelligence and Security Centre'. While a separate cyber service will not be established by the MoD, 'relevant cyber capabilities will be incorporated within the Defence Cyber Command, which will come under the […] management of the […] army'. A broader National Cyber Security Strategy was published in 2011, and a Cyber Security Council was established to coordinate activities and information exchange between the private and public sector in the context of critical infrastructure. A National Security Centre was launched in January 2012. The Netherlands has a national CERT, is involved in informal CERT communities, and is a member of the European government CERTs Group (ECG)." (Military-Balance Online, 2013, p. 73)

Portugal: Atingindo os "mínimos" para manter-se Ciber-confiável?

> "[…] O primeiro passo está dado: a Resolução do Conselho de Ministros 12/2012[159], de 7 de Fevereiro, veio, na esteira das conclusões do **Grupo de Projeto para as Tecnologias da Informação e Comunicação**[160], definir as linhas gerais de uma **Estratégia Nacional de Segurança da Informação (ENSI)** […] A implementação dessa estratégia passará pela criação[161] de um **Centro Nacional de Cibersegurança**,

[159] "Resolução do conselho de Ministros (RCM) nº12/2012 – Plano Global Estratégico de Racionalização e Redução de Custos nas TIC, na Administração Publica (PGERRCTIC): 25 Medidas; 5 Vetores; Período de implementação 2012-2016; Poupança estimadas ~500M€/ano", HONORATO, Manuel "*A Cibersegurança, visão do Estado*" em II Conferência de Hiperíon Cibersegurança em Portugal: Aonde nos encontramos?, Universidade Lusófona – Instituto de Estudos de Segurança/Centro de Gestão da Rede informática do Governo (CEGER)

[160] "Resolução do conselho de Ministros (RCM) nº46/2011 – Criação do Grupo para as Tecnologias de Informação e Comunicação (GPTIC)", Idem.

[161] "O Centro Nacional de Cibersegurança (CNCSeg) foi criado formalmente esta sexta-feira [09/05/2014, quando a CE Europeia tinha exigido a criação destes centros até ao final de Dezembro de 2012.], através de um decreto-lei da presidência do Conselho de Ministros [Decreto-Lei n.º 69/2014

> pela melhoria das condições operacionais do **Sistema de Certificação Eletrónica do Estado (SCEE)**, pelo desenvolvimento de uma solução de **criptografia de origem nacional** e pela **revisão do quadro legal** existente sobre informação classificada, ou seja, dos atuais SEGNAC's. [Segurança de Matérias Classificadas …]" Alocução senhor Ministro da Administração Interna na conferência «O Desafio da Cibersegurança», p.3, 16 de fevereiro de 2012

Interessa descrever (para este trabalho) os ***Objetivos*** da '***Medida 04–Definição e Implementação de uma Estratégia Nacional de Segurança da Informação'*** (das 25 medidas, nos 5 vetores da RCM n.º 12/2012):

- ***'Os objetivos Nacionais para a Segurança da Informação'*** *– Aquilo que cada membro da Sociedade da Informação pode esperar e contar a nível nacional;*
- ***'A Responsabilidade na Segurança da informação'*** *– Quem é o responsável pela implementação da Segurança da Informação no País;*
- ***'Organização da Segurança da Informação'*** *– Qual a estrutura definida para a Segurança da Informação;*
- ***'Gestão'*** *– Quem é o responsável por Estabelecer, Controlar e Medir, Gerir o Risco e Auditar a Segurança da Informação;*
- ***'Serviços de Segurança da Informação'*** *– Que serviços são fornecidos a nível nacional e por quem.*

Interessa, também, enunciar as ***Ações*** previstas da '***Medida 04–Definição e Implementação de uma Estratégia Nacional de Segurança da Informação'***:

- **'*Estrutura Nacional de Segurança da Informação*'** – Revisão e promulgação;
- **'*Centro Nacional de Cibersegurança (CNCSeg)*'** – criação, instalação[162] e operacionalização[163] do Centro;

---

http://www.dre.pt/cgi/dr1s.exe?t=dr&cap=1-1200&doc=20140696&v02=&v01=2&v03=1900-01-01&v04=3000-12-21&v05=&v06=&v07=&v08=&v09=&v10=&v11=%27Decreto-Lei%27&v12=&v13=&v14=&v15=&sort=0&submit=Pesquisar que procede à segunda alteração ao Decreto-Lei n.º 3/2012, de 16 de janeiro, que aprova a orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança], com quase dois anos de atraso em relação às metas europeias e sem autonomia administrativa. A CE Europeia havia definido que até ao final de Dezembro de 2012 todos os Estados membros deviam ter estas estruturas operacionais. A congénere portuguesa, porém, só agora arranca. Além disso, o CNCSeg surge, devido à crise, ainda sem a autonomia administrava que a comissão instaladora daquele organismo defendia. O centro vai, então, integrar o Gabinete Nacional de Segurança (GNS) pelo menos até 2017, altura em que será alvo de avaliação." Retirado de "Centro de Cibersegurança criado com o atraso de dois anos e sem autonomia financeira devido à crise" Consultado em http://www.publico.pt/sociedade/noticia/centro-nacional-de-ciberseguranca-tem-de-criar-medidas-para-reagir-a-ciberataques-1635265 a 17/jun./2014.

[162] "RCM n.º 42/2012 – Criação da CE Instaladora do Centro Nacional de Cibersegurança: 9 Entidades; 4 Personalidades de reconhecido mérito; Equipa multidisciplinar; Presidida pela Autoridade Nacional de Segurança.", HONORATO, Manuel "*A Cibersegurança, visão do Estado*" em II Conferência de Hiperíon Cibersegurança em Portugal: Aonde nos encontramos?, Universidade Lusófona – Instituto de Estudos de Segurança/Centro de Gestão da Rede informática do Governo (CEGER)

[163] "Apresentação do Relatório Final em Junho de 2012: Implementação faseada entre 2013-2015; Dependência Direta do PM; Autoridade sobre entidades do Estado e progressivamente extensível a infraestruturas críticas; Capacidade operacional e de resposta; Competências de autoridade técnica e de doutrina; Interlocutor com entidades estrangeiras congéneres (Nações, NATO, EU, …)", Idem.

- **'*Sistema de Certificação Eletrónica do Estado (SCEE)*'** – aprofundamento e melhoria das condições de operação da SCEE, com vista à sua adequação aos requisitos internacionais mais recentes;
- **'*Criptografia Nacional*'** – criação e certificação de uma solução de criptografia forte de origem nacional, desenvolvimento de soluções para a sua utilização e promoção junto de potenciais utilizadores;
- **'*Revisão do Quadro Legal para a Segurança das Matérias Classificadas*'** – incluindo a salvaguarda da informação classificada, da credenciação pessoal e industrial e ainda da segurança dos sistemas de comunicação e informação, substituindo os SEGNAC's[164].

Quer os objetivos, quer as Ações foram retiradas e adaptadas da apresentação na intervenção de ", HONORATO, Manuel (Comandante de Mar-e-Guerra–CMG e Eng.º de Material Naval, adstrito ao CEGER)"*A Cibersegurança, visão do Estado*" em II Conferência de Hiperíon Cibersegurança em Portugal: Aonde nos encontramos?, Universidade Lusófona–Instituto de Estudos de Segurança/Centro de Gestão da Rede Informática do Governo–CEGER, cf.. O ponto 4.4 do Anexo da RCM n.º 12/2012 publicado na p. 598 no DR, Iª série- N. 27–7 de fevereiro de 2012

A questão que se coloca sobre o Centro Nacional de Cibersegurança–CNCSeg é a seguinte: Se o Centro se destinava a funcionar integrado no GNS, por razões de ordem económicas e orçamentais[165] –que até se compreendem–, qual(ais) a(s) razão(ões) que levaram a Comissão Instaladora[166] do CNCSeg e/ou os decisores políticos [e/ou militares] a prolongar(em) a situação formal de entrada em funcionamento, colocando

---

[164] "Resolução do Conselho de Ministros n.º 50/88: Aprova as instruções sobre a segurança de matérias classificadas (SEGNAC). Declaração da Secretaria-Geral da Presidência do Conselho de Ministros: De ter sido rectificada a Resolução n.º 50/88, que aprova as instruções sobre a segurança de matérias classificadas (SEGNAC), publicada no Diário da República, 1.ª série, n.º 279, de 3 de Dezembro de 1988 Altera as instruções para a segurança nacional, salvaguarda e defesa das matérias classificadas (SEGNAC 1), aprovadas pela Resolução do Conselho de Ministros n.º 50/88, de 3 de Dezembro Resolução do Conselho de Ministros n.º 37/89: Aprova as normas para a segurança nacional, salvaguarda e defesa das matérias classificadas, segurança industrial, tecnológica e de investigação - SEGNAC 2. Resolução do Conselho de Ministros n.º 16/94: Aprova as instruções para a segurança das telecomunicações (SEGNAC 3). Resolução do Conselho de Ministros n.º 5/90: Aprova as instruções sobre a segurança informática (SEGNAC 4)." Consultado em http://www.cfsirp.pt/Geral/segnac.html a 23/jun./2014.

[165] "Como o Programa do XIX Governo Constitucional, o atual contexto económico e financeiro do País e o disposto na Lei n.º 83-com2013, de 31 de dezembro, desaconselham a criação de novos serviços públicos, considera-se qie o aproveitamento das sinergias de um serviço já existente, especialmente em matéria de instalações e equipamentos, constitui a solução mais adequada para a criação, instalação e operacionalização do CNCSeg." Decreto-Lei n.º 69/2014, publicado no diário da República, 1.ª série – N.º 89 – 9 de maio de2014.

[166] "O Governo aprovou hoje [5 de abril de 2012] em Conselho de Ministros a criação da comissão instaladora do Centro Nacional de Cibersegurança. Até 30 de junho [de 2012] este organismo terá de apresentar um relatório com o "modelo e todas as medidas e instrumentos necessários à respetiva implementação", detalha a nota de imprensa que resume os pontos aprovados na reunião ministerial desta manhã." Consultado em http://tek.sapo.pt/noticias/computadores/centro_nacional_de_cibersegurança_com_modelo_1234112.html a 17/jun/2014.

Portugal em incumprimento das *deadlines* da Agenda Digital que deveriam ter sido implementadas até 31 de dezembro de 2012, diminuindo a ciber-confiabilidade do País perante os parceiros da UE e, de forma indireta, da OTAN?

As respostas poderão ser variadas e até justificadas, e o *timing* da implementação desvalorizado –de até 2016 passará para 2017–, mas a "linha de pensamento" que sobressai é a de que poderia ter sido feito o mesmo –a integração do CNCSeg no GNS– em, muito, menos tempo[167], cumprindo os prazos. «A dúvida é/[era] se se deve criar /[se devia ter criado] uma nova estrutura ou aproveitar as já existentes» que já vinha de 2011. Com isso, tinha-se contribuindo para a melhoria do estatuto do País, ao nível da ciber-confiabilidade, não permitindo, que o mesmo possa, apesar da "expressão-reduzida", dos problemas orçamentais, económicos, financeiros, etc., atingir uma posição de vulnerabilidade de *EU-NATO-Cyber persona non grata*.

Uma outra questão que tem surgido no "horizonte" –em vários fóruns, seminários, palestras, artigos de opinião[168] e trabalhos na Academia, etc[169], relacionados com o campo da Cibersegurança em Portugal– dizem, invariavelmente, respeito às

[167] "[…] entende-se que o GNS é o serviço indicado para albergar o CNCSeg na fase inicial do seu funcionamento, modelo que, contudo, será objeto de avaliação no final do ano 2017, período que se antecipa necessário para a completa estruturação e funcionamento em cruzeiro do referido Centro, com vista a uma decisão sobre a manutenção do arquétipo agora definido ou a evolução para uma completa autonomização do CNCSeg." Idem, Decreto-Lei n.º 69/2014, publicado no diário da República, 1.ª série – N.º 89 – 9 de maio de2014.

[168] "[…] Em Portugal, as estruturas militares parecem estar preparadas para este cenário e seguem de perto as recomendações da OTAN. Sousa Pereira, do Estado-Maior General das Forças Armadas (EMGFA) lembrou que em 2008 foi criado o CRISI – Capacidade de Resposta a Incidentes de Segurança Informática nas Forças Armadas e o grupo de resposta GRISI, a servirem o EMGFA e os Estados Maiores da Armada, Exército e Força Aérea. No primeiro ramo, Pereira Simões fala do 'caminho a seguir', com a necessidade de 'alinhamento de políticas, normas e procedimentos', definição de 'capacidade conjunta' e 'cooperação e partilha de informação'. Viegas Nunes assegura que o Exército já possui 'capacidade ofensiva e também defensiva na sua estrutura' e os seus objetivos estratégicos estão inscritos numa «Visão para a superioridade da informação'. Também a Força Aérea, segundo Paulo ALVES, já viu promulgada a sua 'Política de Ciberdefesa'. Mas, quando a OTAN lhe perguntou qual a entidade coordenadora da ciberdefesa em Portugal, Torres SOBRAL 'não soube responder'." *"Quem manda na cibersegurança em Portugal? Ninguém."* , publicado a 03/05/2011, consultado em http://www.computerworld.com.pt/2011/05/03/portugal-se-estrategia-coordenada-de-ciberseguranca/, a 16/jun./2014.

[169] "Conclusões (GPTIC): - Portugal em 2005 era vanguarda na Europa e na NATO para a criação de um ENSI, em 2012 é um dos países mais atrasados nesta matéria; A abrangência deverá extravasar o Estado, englobando toda a sociedade da informação e Infraestruturas Críticas; A ENSI de 2004/2005, após 7 anos, continua a ser bastante atual requerendo uma revisão para a adptar a novos cenários de ameaça e aos novos conceitos de segurança; - Centro Nacional de Cibersegurança (CNCSeg), não é uma opção, é uma obrigação de Portugal perante os seus pares e uma necessidade de sobrevivência; - Modelo do CNCSeg, …" …)", HONORATO, Manuel "*A Cibersegurança, visão do Estado*" em II Conferência de Hiperíon Cibersegurança em Portugal: Aonde nos encontramos?, Universidade Lusófona – Instituto de Estudos de Segurança/Centro de Gestão da Rede Informática do Governo (CEGER)

«ausências» de estratégia(s)[170] [171]. «[… Quem] deve dar resposta ao que proteger[172], ao que valorizar na proteção[173], analisar as causas de impedimentos à segurança e confiabilidade e como fazer [a procura de soluções].» (CALDAS & FREIRE, 2013, p. 9) na organização funcional de «comando e controlo» da Cibersegurança no País[174]?

Relativamente a outros EMs da UE de dimensão similar, despendendo recursos semelhantes e adotando "figurinos" de integração da Cibersegurança em estruturas já existentes –como o caso específico da Holanda– a diferença entre os dois países é imensa: A Holanda vai na segunda revisão da sua ECS e Portugal nem vai na versão *Beta* (pelo menos que seja do conhecimento público, não contando com a proposta disponível em http://www.gns.gov.pt/media/1247/PropostaEstratégiaNacionaldeCibersegurançaPortuguesa.pdf , consultada a 23 de junho de 2014, porque não implementada ou estando em fase de teste. Uma proposta, segundo notícia de 2 de julho de 2014, foi entregue ao Governo;

[170] "A estratégia, enquanto elemento aglutinador, é a materialização num plano de ação das orientações, das ações e das prioridades. É extremamente simples traduzi-la em legislação bastando quase 'decalcar', com as devidas adaptações, por uma das estratégias de entre os 13 países[* **] que já publicaram as suas. A essência do problema parece-nos estar mais na capacidade de envolvimento da sociedade para esse fim comum e na racionalização de investimentos. A estratégia para além de ter de envolver aspetos políticos, o governo deve ter a esse nível uma visão macro dos problemas sem esquecer a objetividade de criar mecanismos para os resolver. Só faz sentido ser implementada, se equacionar a solução dos problemas de modo completo e com eficácia. No mundo real, o que verdadeiramente está em causa é a segurança – relativamente a ameaças intencionais e intrusivas – e a confiabilidade – assegurar o funcionamento mesmo contra ameaças e desastres acidentais – de algo materializável: a informação (propriamente dita) e as infraestruturas de informação (sistemas e redes) [*]Sinónimo da urgência e da relevância que a temática lhes merece são já 13 os países com Estratégias de Cibersegurança, a saber: África do Sul, Alemanha[*DE*], Austrália [Au], Canadá [Ca], Estónia[*EE*], EUA, França[FR], Holanda[*NL*], Japão, Nova Zelândia [NZ], Reino Unido[*UK*], República Checa e Polónia. [**][Depois da publicação outros Países já o fizeram, como por exemplo e no que a este trabalho interessa, Finlândia/FI, Eslováquia, Hungria, Lituânia, etc., fonte consultada em http://www.gns.gov.pt/new-ciberseguranca.aspx a 23/jun./2014.]" (CALDAS & FREIRE, 2013, p. 9)

[171] "A necessidade de um Centro Nacional de Cibersegurança foi focada por várias entidades. Antero Luís, Secretário-geral do Sistema de Segurança Interna (SSI), considera necessária uma estratégia nacional 'que não pode ser diferente da de outros países', que passa por dois níveis, um estratégico e outro tático." Idem *"Quem manda na cibersegurança em Portugal? Ninguém."* , publicado a 03/05/2011, consultado em http://www.computerworld.com.pt/2011/05/03/portugal-se-estrategia-coordenada-de-ciberseguranca/, a 16/jun./2014.

[172] "O que proteger aponta para os ativos (inclui a informação) segundo uma lógica de criticidade na perspetiva da natureza (digital ou físico, informação ou infraestrutura), de tipificação (público, privado, militar, …) e de impacto geográfico (local, [regional], nacional, …)." (CALDAS & FREIRE, 2013, p. 9)

[173] "O valor é encarado na cadeia – valor organizacional dentro da instituição e na sua (inter)dependência com outras – e em termos operacionais – funcionamento do sistema e por conseguinte confiabilidade técnica." Idem (p. 9)

[174] "O presente *working paper* tem por objetivo sensibilizar para a necessidade de adotar urgentemente medidas de cibersegurança a nível nacional, nomeadamente no que respeita à atribuição e definição da liderança do processo, à organização/sistema em que deve assentar a coordenação e implementação e, ainda, quanto à definição de uma estratégia que dê as orientações para as ações a desenvolver." Idem (p. 1)

http://www.ionline.pt/artigos/portugal/estrategia-nacional-ciberseguranca-entregue-ao-governo/pag/-1 , consultado a 19 de outubro de 2014. Segundo este autores, «Portugal está 'muito frágil' em medidas de Cibersegurança numa perspetiva de resposta liderada, estruturada e sujeita a entidades organizacionais.» (CALDAS & FREIRE, 2013, p. 16)

1.5 Os Direitos dos Cidadãos, a Privacidade e a Proteção de Dados

> "**Protecting fundamental rights, freedom of expression, personal data and privacy**- Cybersecurity can only be sound and effective if it based on fundamental rights and freedoms as enshrined in the Charter of fundamental rights of the European Union and EU core values. Reciprocally, individuals' rights cannot be secured without safe networks any systems. Any information sharing for the purposes of cyber security, when personal data is at stake, should be compliant with EU data protection law and take full account of the individuals' rights in this field." (HIGH REPRESENTATIVE/VICE PRESIDENT, 2013, p. 4)

> "[…] It aims to foster national security without compromising democratic prinCIPles or unduly violating individual liberties. However, it is hard to find a balance between these goals, and the EU´s measures thus inevitably raise questions about the democratic implications of European cyber security policy: are the institutional structures and instruments of European cyber security policy compatible with the criteria of democratic governance?" (BENDIEK, "European Cyber Security Policy", 2012, p. 1)

Os tópicos presentes nesta seção são de sobremaneira importantes no Ocidente, em geral, e na Europa, em particular. Estão, intrinsecamente, ligados à matriz de Valores das sociedades democráticas. Não será de estranhar que, os mesmos, tenham estado presentes –nos últimos anos– nas preocupações das Organizações não Governamentais (ONG/*Non-Governmental Organizations–NGO*) ligadas aos Direitos Civis, dos cidadãos enquanto indivíduos esclarecidos, das instituições judiciais e até políticas, apesar do contexto de crise financeira, económica e social que temos vindo a atravessar. Isto é válido para as duas "margens" do Atlântico, com algumas diferenças em relação ao "centro de gravidade". Enquanto, que, nos Estados Unidos este conjunto de preocupações não é generalizado na população americana, na Europa do centro e norte, em particular, são-no por razões culturais intrínsecas e de longa data. Não quer dizer que a Nação americana, democrática, –com o seu sistema de *checks and balances*– não contribua para a sua implementação e verificação sistémica, vindo a fazê-lo através das organizações de Direitos Cívicos da Sociedade americana, por exemplo, a *Electronic Privacy Information Center–EPIC* [175] [179](www.epic.org, consultado a 23 de fevereiro de 2013) e as vinte e duas Associações Americanas de Consumidores, que

dirigiram uma missiva aos *MEPs* a 17 de outubro de 2013, que indicava as preocupações do lado de lá do Atlântico relativamente a assuntos de Proteção de Dados:

> We are writing to you on behalf of US consumers to express strong support for the new European Union Data Protection Regulation. Many of us wrote to you last year at this time to express our support and to offer specific suggestions. As we explained, 'we believe that the promotion of stronger privacy standards in Europe will benefit consumers around the globe.'" consultado a 23 de junho de 2014 em http://www.consumerwatchdog.org/resources/ltreudatareg101513.pdf

As preocupações com este tipo de assuntos nos EUA fundamentam-se mais no sistema judicial e cívico[175] –de apoio à economia que, verdadeiramente, funciona[176]–, e nas associações de Direitos do Consumidor, que com o cidadão comum, que tem outras preocupações, mais imediatas, no seu dia-a-dia no frenético desafio do *make-business*, não querendo isto dizer que o cidadão europeu não tenha as mesmas preocupações, muito pelo contrário, mesmo antes da crise. Por outro lado, o quadro de referência dos Direitos Fundamentais apela mais ao cidadão comum europeu do que ao americano, talvez, devido ao que resta do sistema social europeu, à matriz da própria sociedade europeia mais consentânea com uma certa tradição cultural Humanista clássica, etc.

Podem-se definir, pelo menos, três planos relativos às preocupações com este tipo de assuntos: o internacional, o transatlântico e o interno da UE. Quanto ao primeiro poder-se-á dizer que era inevitável o aumento da pirataria, como já vimos, do roubo da propriedade intelectual, a fraude dos dados pessoais de cidadãos europeus, etc., não só

[175] "European High Court Strikes Down Data Retention Law: In a far-reaching and dramatic opinion, the European Court of Justice has ruled that the mass storage of telecommunications data violates the fundamental right to privacy and is illegal. The Data Retention Directive required telephone and Internet companies to keep traffic and location data as well as user identifying information for use in subsequent investigations of serious crimes. According to the Court, the Directive imposed "a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary." The Court found that the collection of metadata constitutes the processing of personal data and must therefore comply with Article 8 of the Charter of Rights. The Court also said to find a privacy violation, "it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way." Last year EPIC, joined by dozens of legal scholars and former members of the Church Committee, urged the US Supreme Court to find the NSA's telephone record collection program unlawful. For more information, see EPIC - Data Retention, In re EPIC. (Apr. 8, 2014) http://epic.org/privacy/intl/eu_data_protection_directive.html consultado em 11/jul./2014.

[176] "The US approach is more sectorial in nature, with highly effective enforcement in those sectors by organizations such as the Federal Trade Commission. Class-actions in relations to privacy infractions are also an important driver of good data practices in the US. Recently attending a conference in US, I was struck by the fact that the good practice advice from panels was not very different from what you would hear at a European event. The difference was that he main driver was not prescriptive law in Europe but the financial and reputational risk arising from class-actions." (HAWKES, 2014, p. 5) O texto da intervenção poderá ser obtido em http://www.iiea.com/event/download_transcript?urlKey=keynote-address-billy-hawkes a 27/jul./2014.

devido à Globalização, mas também devido à necessidade de desenvolvimento –a qualquer custo– das sociedades (re)emergentes[177], algumas delas autoritárias, outras teocráticas e outras, até, democráticas. Até se poderia considerar "normal", algum tipo de espionagem (*CNE*) levado a cabo por algumas delas e apropriação direta de dados dos EMs (e indireta de cidadãos desses estados europeus), pelo "princípio da reciprocidade"[178]. Igualmente no espaço transatlântico, também devido à Globalização, era inevitável a pressão das multinacionais americanas em relação aos direitos de propriedade intelectual das empresas e dos direitos e dados de cidadãos europeus, pelo «controlo extraterritorial de conteúdos e acesso a dados» (LOSEY, 2014, p. 85). Não era previsível, no entanto, que após os acontecimentos do *9/11* e de toda a colaboração e solidariedade que foram prestadas pela Europa –com a agravante, dos países visados, na sua maioria pertencerem à OTAN–, o comportamento dos EUA nesta matéria. Quer de ambas as Administrações Republicanas BUSH em geral, mas acima de tudo, da postura das Administrações Democráticas de Barack OBAMA e em particular da, segunda, atual. Das duas, uma: ou o atual Presidente OBAMA foi "ludibriado" por resquícios das Administrações anteriores, uma vez que teve o tempo suficiente –durante o primeiro mandato– para corrigir e reverter a situação, supostamente, herdada), ou, de certa forma, foi conivente, logo primeiro responsável, com a situação –aguda, interna[179] e embaraçosa de «quebra de confiança»[180], externa– de "vigilância generalizada" de cidadãos anónimos inocentes e de políticos de países "amigos" –nomeadamente,

[177] "To be sure, economic historians remind us that in fact Asia had been the predominant producer of the world's total GDP for some eighteen centuries. As late as the year 1800, Asia accounted for about 60% of the world's total GDP, in contrast to Europe 30%. India's share alone of the global product in 1750 amounted to 25% (according to Jaswant Sigh, former Indian finance minister), much like that of the United States today. But during the nineteenth and twentieth century's, with the intrusion of European imperialism backed to Europe's surging industrial innovation and financial sophistication, Asia's global share declined precipitously. By 1900, for example, under prolonged British imperial rule, India's share shrank to a more 1.6%" (BRZEZINSKI, 2012, p. 15)

[178] "Espionage in a cyber context is a vexing issue. All states engage in the clandestine acquisition of confidential intelligence from other actors. The digital age has neither created nor changed this goal." (MUELLER, 2014, p. 8)

[179] "Atendendo às questões levantadas nos EUA sobre a implementação da ciberestratégia relacionadas com os direitos cívicos, nomeadamente as recentes tentativas de fazer aprovar o *Cyber Security Act* de 2012, ou *Cyber Intelligence Sharing and Protection Act* (CISPA) de 2013, – aprovadas no Câmara dos Representantes mas recusadas no Senado – e a implementar a *Presidential Policy Directive 20*[*] (PPD 20, tornada pública após intervenção do Electronic Privacy Information Centre EPIC[*]. [*]"The U.S. House of Representatives has passed the controversial Cyber Intelligence Sharing and Protect Act (CISPA) by a vote of 288 to 127, RT reports. Read more: http://www.businessinsider.com/congress-passes-cispa-cybersecurity-bill-2013-4#ixzz2X8OLZajJ " consultado em 23 de junho de 2013.

[180] "The revelations of Edward SNOWDEN have opened a breach of trust between the United states and Europe that will not be closed easily or quickly.[…]" (MASCOLO & SCOTT, 2013, p. 2)

europeus– levada a cabo pela *NSA* e, supostamente, com o apoio de outros serviços de inteligência europeus (*UK*). No plano da Segurança interna da UE, vislumbra-se a necessidade de um balanceamento articulado entre as reais necessidades de "securitização"[141] das políticas de Cibersegurança por um lado, e os Direitos Fundamentais dos Cidadãos e os Valores Nucleares da UE por outro, como vimos nas citações que deram o mote a esta seção. A primeira "prova-de-fogo" deste balanceamento está nas agendas política da UE através de várias frentes:A rejeição da '***European Data Retention Directive'–EUDRD*** por parte do TdJ[181], após a rejeição do Tribunal Constitucional Alemão e de dúvidas pertinentes de outros Tribunais de vários EMs, nomeadamente do Supremo Irlandês[182] –devido à sua exposição a algumas multinacionais de peso, *Microsoft, Apple, Google Europe*[*] e *LinkedIn Europe*[*]– sedeadas[*] e a operar na Irlanda, derivada de uma interpretação "mais *soft*" –em relação a outros EMs da UE– sobre a Diretiva de 1995, 95/46/EC[LRG0A] [183], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML , consultada a 10 de junho de 2014. Existe legislação aprovada e em vigor nos EMs que terá de ser revogada "à luz" da nova decisão. E há jurisprudência e decisões tomadas que terão de ser, pelo menos, reanalisadas; O Pacote da Reforma da Proteção de Dados ***´Data Protection Reform Package Lesgilation'–DPReform,*** indexado por COM(2012) 9 final[LRG110] de 27 de janeiro de 2012 e intitulado '*Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21th Century*' e cuja iniciativa data de há, pelo menos, quatro anos e meio. Na proposta de composição, optou-se: por uma Regulamentação, a ***´General Data Protection Regulation'–GDPR*** destinada a

[181] Press release of the Court of Justice available under http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf) Full text of the Decision available under http://curia.europa.eu/juris/documents.jsf?num=C-293/12.)" em http://www.mondaq.com/x/306158/Data+Protection+Privacy/EU+Data+Retention+Directive+declared+null; consultado a 19/abr./2014.

[182] "The resulting debate has thrown a welcome spotlight on the general issue of State access to personal data. The recent decision of the EU Court to invalidate the Data Retention Directive has clearly set out the need for proportionality in this area. The lack of such proportionality led my predecessor, Joe MEADE, to take enforcement action against the initial Irish data retention regime, action that has now been vindicated by the European judgment. The judgment also shows the importance of challenging such privacy-destroying measures, as was done in this case by a nongovernmental organisation, Digital Rights Ireland, supported by the Irish Human Rights Commission. It now falls to the High Court, which referred the case to the EU Court, to take account of the judgment in its consideration of the Irish data retention legislation." (HAWKES, 2014, p. 1) O Sr. HAWKES é o responsável pela Autoridade de Proteção de Dados da Irlanda.

[183] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *Official Journal L 281 , 23/nov./1995 P. 0031 – 0050*"

nivelamento padrão e harmonização comunitária europeia –'*Proposal for a regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such a data';* e, uma Diretiva destinada ao Sistema Judicial –*LEA*–, *'Proposal for a directive of the European Parliament and the council on the protection of individuals with regard to the processing of personal data by competente authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalities, and the free movement of such data'*. Do total de tempo, dois anos foram de extenso, complexo e profícuo trabalho por parte da CE, nomeadamente da Comissária Viviane REDING, do Luxemburgo, responsável nos últimos anos pelo ***DG JUSTICE***, e dois e meio da comissão *LIBE* do anterior PE[184] –cerca de 4000 recomendações à legislação emanada da CE–, que "correm" um sério risco de ter sido em vão; Devido às últimas denúncias de atividades de serviços de inteligência de países exteriores –adversários e aliados– e de, alguns, EMs da UE, do incremento de ameaças de [ciber]terrorismo ideológico e religioso, não seria de estranhar a necessidade de incrementar as proteções de [ciber]segurança nos vários EMs, o que poderia conduzir a um aumento de "securitização"[141] das políticas relativas à segurança em geral e do Ciberespaço em particular de cada um deles e, por associação, da própria União. Este tipo de procedimentos, poderão conduzir a uma redução dos Direitos Fundamentais dos Cidadãos, se os Parlamentos nacionais e Europeu não tiverem a sua participação democrática nestes processos políticos[185]; E, como consequência dos anteriores, como será possível a UE propalar na sua ECS a convicção inabalável nos Direitos Fundamentais dos Cidadãos –quer *off-line*, como *on-line*– como suporte à sua PESC e projeção de *SoftPower*, se tem permitido a sua redução interna, por razões de segurança,

[184] "[…] We had at this point, what the LIBE Committee has done, really, a great job. Preparing the result out of the 4000 amendments – we can, sometimes disagree with parts of things that was done there, but, I have to say, that I admire the work that was done in the Parliament (EP). Because, I never expected that they can go out of this 4000 amendments with the agreement of all the parties in the Parliament (EP)." Wojciech WIEWIÓROSKI, GIODO (PL), Polish Data Protection Authority (DPA) 13':45"
CPDP 2014: EU Data Protection Reform: State Of Play, CPDP Conferences Organised by CPDP Chair: Christopher Docksey, EDPS (EU) Moderator: Nikolaj NIELSEN, EU Observer (BE) Panel Anna FELDER, Privacy International (UK), Paul NEMITZ, EC DG Justice (EU), Philippos MITTLETON, Permanent Representation of Greece (GR), Wojciech WIEWIÓROSKI, GIODO (PL)

[185] "The constructive role of national parliaments in the institutional and material regulation of European cyber security policy is of particular importance, as parliaments as responsible for the communication with the general public. In democratic structures, parliaments should be the place where the relationship between security and freedom is being defined – especially when it comes to cyber security policy." (BENDIEK, "European Cyber Security Policy", 2012, p. 6)

e externa como sacrifício de crescimento económico a qualquer preço, concretamente, na venda de ferramentas digitais de controlo de conteúdos[186] e nas negociações –pouco transparentes (como aconteceu com o *Anti-Counterfeiting Trade Agreement–ACTA*)[187], como reflexo do *Stop On-line Piracy Act–SOPA* e do ***PROTECT IP Act*** ou *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act–PIPA* (SCHAAKE, 2013, p. 01':50")[186], nos EUA– em aspetos fulcrais, quando assuntos delicados continuam pendentes relacionados com os acordos *Safe Harbour*[188] [189], *o Investor-to-State Dispute Settlement–ISDS*[190] e parece estar a acontecer com o *TTIP*.

---

[186] "Secondly, in Europe we need have our house in order to be a credible advocate in digital freedoms globally and this is in our interest. The big debate about Data Protection Privacy and Digital Freedoms follow in the NSA revelations is timely and necessary. Something have missing from the discussion is the role of the European Technologies play in facilitating such massive surveillance programs. In fact, European companies are in front rumors in developing, exporting and employing the very tools and technologies used for mass surveillance, monitoring, mass censorship, hacking, tracking and tracing and the some goes for software vulnerabilities or 'zero-day' exploits" (SCHAAKE, 2013, p. 3':45") https://www.youtube.com/watch?v=u6rd3qvXJFQ, acedido a 05/ago./2014

[187] "The negotiations over the International Convention on the Anti-Counterfeiting Trade Agreement (ACTA) made it clear that exclusive, opaque politics will lead to no results. Non-governmental groups such as representatives of the Internet industry, the civil society or the technical community should be included in political decision-making process. This way, European coordination would follow the established principles of the internet culture: it would be 'open', not 'closed', 'bottom up' instead 'top down' and 'inclusive' not 'exclusive'." (BENDIEK, "European Cyber Security Policy", 2012, p. 6)

[188] "Q: […] That now to slide a related issue and is that of the *Safe Harbor*, which is the agreement between the European Union (EU) and the United States (US), where the US companies signed-up, saying the promise to protect the EU citizens data. Now, we have heard a lot of talk about, 'that it does not working very well', and certainly the Parliament is said, perhaps should be suspend. What is your view on that? A: Well, we have analysed *Safe Harbour*, which is a gift wish the EU makes to the US, because the US does not have Data Protection rules. So, in order nevertheless to give their companies the possibility to exchange commercial data, that the *Safe Harbour* scheme was been created. Now, I have been analysed and that are not looking very safe, I must say, and for this, why I gave to the American counterparts, to the Government, thirteen «point to-do-list» to be completed by summer. I have to see if that «to-do-list» is completed it is fine. That means the *Safe Harbour* can be safe again. If not, well, than now I will be discuss this with the Parliament and as you know, the Parliament wants, simple, to scrap *Safe Harbour* [agreement]." Aos 02':14". Leading ICT journalist Jennifer BAKER is joined by Viviane REDING, European Commissioner for Justice, Fundamental Rights & Citizenship, to discuss data protection regulation and the EU-US Safe Harbor agreement. Em http://www.vieuws.eu/ict/safe-harbor-reding-warns-us-that-progress-is-needed-before-summer/ obtido a 26/mar./2014.

[189] "On the second question of *Safe-Harbour*, here the draughts were the Commission will be able to work with US to implement what we have put out in terms of 13 recommendations for improvements. And I can take notes of this doubts – I am, myself, the chief negotiator with the US on this – and I would do my best. And, I am confident that we will be able to implement this recommendations, because my feelings as: the people in the US, they also believe in freedom, they believe in the protection of the individual life, or they identity. Americans do not want to be spied also on that they want to have Data Protection. They are a great country on Democracy with a free press and great individualism, and they have a vibrant Civil Society and know working in Democracy. [And] I am confident then when we work together with them, they will be convinced conversion in the future of how we will be doing privacy and progress of the *Safe-Harbour* will be the some type of, not only the symbol, but relevant of this progress as the speech of the President OBAMA of Friday and the policy instructions, on protecting privacy also of people in another countries were a first step in create a sigh that this were the thing are going. This is the only one way when privacy protection on both sides of the Atlantic. The digital future and that is

A Lei de Retenção de Dados e as suas consequências na União Europeia

Reforma da ***EUDRD***[191] obriga os operadores de telecomunicações e os Fornecedores de Serviços de Internet (FSI/*Internet Service Providers–ISP*) a "reterem" os dados de comunicação, ou melhor os "meta-dados"[TD&T16] –dados relativos à comunicação propriamente dita e não ao seu conteúdo. Mas devido ao desenvolvimento tecnológico e em determinadas situações seria possível correlacionar algo mais que isso, podendo-se decifrar algum conteúdo–, dos seus subscritores e assinantes por um período, pelo menos, de seis meses. Se os operadores de telecomunicações já o faziam para efeitos de faturação, os *ISPs* não. Assim que a Diretiva foi sendo transposta para a legislação dos vários EMs, isso obrigou a avultados investimentos de processamento, mas acima de tudo, de armazenamento de informação. O objetivo da Diretiva era claro: reconstruir, se necessário, cenários de relações de autores ou aceitadores –voluntários ou não– de comunicações eletrónicas de dados e de voz, fixas ou móveis. O princípio político era "nobre", se estes "meta-dados"[TD&T16] fossem só utilizados para procedimento criminal sob supervisão judicial. O problema surge quando os serviços de inteligência passaram a utilizar estes dados para outros fins, que não, os de aplicação expressa de ordem judicial. É um procedimento comum, atualmente. Os serviços de

---

more of it and I think more and more people in America, including in the Government understand and let it is make my confident that on the SH we will be able to make good progress and come back with the results against the doubts which are fair to have today. " NEMITZ, Paul, Representante do DG JUSTICE aos 41':24" 7th International Conference – 22, 23 and 24 January 2014, Brussels, Belgium - Computers, Privacy and Data Protection - Reforming Data Protection: The Global Perspective, CPDP 2014: EU Data Protection Reform: State Of Play, que pode ser obtida em https://www.youtube.com/watch?v=kl8an9Myrek; Consultada em 08/ago./2014.

[190] Consultar "*ISDS and TTIP – A miracle cure for a systemic challenge?*", PARDO, Romain – Policy Brief – European Policy Centre, 14 July 2014. Consultado a 17/jul./214 em http://www.epc.eu/pub_details.php?cat_id=3&pub_id=4637

[191] "In the wake of the London and Madrid terror attacks, the European Data Retention Directive (EUDRD) was passed by the Council in 2007. This directive requires all Member States to have legislation in place to ensure that the communication companies and Internet Service Providers (ISPs) maintain records on user traffic (on connections, not however on content) for a maximum of two years." (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 30) CF. "[…] attempts by the EU to impose a directive on data retention met with strong resistance in Germany. The Federal Constitutional Court rejected the German Federal Diet´s (Bundestag) measures transposing the EU directive by arguing that these infringed the right to secrecy of telecommunications (for a more detailed discussion on this case, see the section 'Securitization')" (BENDIEK, "European Cyber Security Policy", 2012, p. 8) e "The data retention directive considerably limits the citizens' right to informational self-determination. Originally, it was meant to be transposed into national law by September 15, 2007. Accordingly, Germany delivered a list of agreed transposition measures to the European Commission in 2008. However, the implementation process was stopped by the Federal Constitutional Court in 2010. Accordingly to the Court, the laws to implement the directive infringed the fundamental right to secrecy of telecommunications. This difference of opinion should well lead to a conflict between the Commission and the Federal Constitutional Court in the future." (BENDIEK, "European Cyber Security Policy", 2012, p. 22) CF. com a nota de rodapé n.º 48, p. 11.

inteligência e informações –em particular na americana *NSA*– recorrerem a bases de dados de empresas[192] para efetuarem as suas análises e investigações, uma vez que, tinha vindo a ser cada vez mais oneroso e difícil criar e manter, atualizadas, bases de dados proprietárias e específicas para os fins em vista –embora, se possa admitir que muitos deles continuem a "gerir" as suas próprias bases de dados, dependendo dos orçamentos disponíveis e da dimensão do país ou EM, em questão, das suas ambições de soberania e da necessidade de projeção exterior. O problema agravou-se quando foi sendo conhecido, aqui e ali, brechas ou falhas no armazenamento e proteção destes «meta-dados» –dados padrão que permitem definir outros dados ou a sua estrutura– por parte dos controladores e fornecedores. Foi perante este cenário, que começaram a crescer as reticências em relação à *EUDRD*. Primeiro, foi o Tribunal Constitucional da Alemanha[193]. Depois, foram Associações de Direitos Cívicos em vários EMs e por fim o escândalo da "vigilância generalizada" e da sua associação com multinacionais americanas que, supostamente, "permitiram" - ou sofreram intrusões das organizações de segurança do seu próprio Governo, *NSA*, da unidade *Tailored Access Operations– TAO*, no acesso aos dados de empresas e cidadãos europeus por parte dos serviços de inteligência de pelo menos, da margem de lá do Atlântico[194]. No entanto, não se exclui de todo que procedimentos análogos não tivessem sido permitidos do lado Europeu, muito em particular, no espaço insular europeu, nomeadamente Britânico, quando, alegadamente, o *GCHQ* -mais especificamente a unidade *Network Analysis Centre– N.A.C.*- infiltrou-se premeditadamente na *BelgaCom*, para aferir a sua eficiência operacional numa empresa dum outro EM da UE e da OTAN).

---

[192] "[…]in particular that Secret Services who rely on data transfers from private parties, which, of course, is the 'business model' of the United States NSA, that is the combination of Public Power combined with these private enterprises, which is uniqueness of the US-NSA model […]" NEMITZ, Paul, Representante do DG JUSTICE aos 31':36" 7th International Conference – 22, 23 and 24 January 2014, Brussels, Belgium - Computers, Privacy and Data Protection - Reforming Data Protection: The Global Perspective, CPDP 2014: EU Data Protection Reform: State Of Play, que pode ser obtida em https://www.youtube.com/watch?v=kl8an9Myrek; Consultada em 08/ago./2014.

[193] "[…] In similar encounter, attempts by the EU to impose a general directive on data retention in Germany encountered strong opposition from both civil society and the Federal Constitutional Court, the latter of which expressed fear that the directive incurred excessive intrusion into postal and telecommunications, as well as the informational self-determination of the individual." (BENDIEK & PORTER, European Cyber Security within a Global Multistakeholder Structure, 2013, p. 159)

[194] "The revelations have provoked a long-overdue debate on the proper balance in a democratic society between the protection of personal data and the obligation on government to take measures against those who would use these services to further criminal objectives. The disclosures have already led to commitments by the US Administration in relation to the activities of US intelligence services." (HAWKES, 2014, p. 1)

A Reforma da Legislação de Proteção de Dados

A *DPReform*[195] teve o seu início, como já foi referido, há quatro anos e meio. No entanto o *draft* da *CE* apresentado ao PE só aconteceu há dois anos e meio. Durante estes últimos anos, foram analisados contributos da Sociedade Civil e dos próprios *MEPs*. O Comité *LIBE* ficou responsável por compilar as contribuições, discuti-las no seu seio e torna-las viáveis, melhorando ou alterando as apresentadas pela CE[196]. Ficou, igualmente, com a responsabilidade política de que fosse possível um consenso de base alargada entre os principais grupos e partidos políticos europeus com assento no PE que terminou funções em junho. O trabalho[197] foi «duro», exigente, complexo, mas foi possível chegar-se a um resultado objetivo e de consenso alargado, tendo sido aprovado pela maioria dos MPEs. Este projeto, após a intervenção do PE foi devolvido à CE com as alterações sugeridas e aprovadas pelos euro parlamentares. De seguida, o *DG JUSTICE* começou o seu trabalho com o Conselho. No entanto desta vez, este trabalho não tem sido fácil. Muito pelo contrário, tem-se notado uma animosidade por parte dos

[195] "Today, we are talking about the Data Protection Reform. Joining me to look into the details of that is the Dutch MEP Sophie In't VELD. Thank you very much to be in here. Q: Commissioner Viviane Reding has separated the new data protection rules into a new regulation for general practices and that the Directive for Law enforcement. Do you think this is the right approach? A: No, I don't think so. We very much wanted a single instrument. I think it would have been Commissioner REDING personal preferences as well. A single standard for Data protection regards of the end users data, and of course, you can't always specifies for you know polices as different from companies or social networks, but we certainly recognize the Police Judiciary and Intelligence Services are no longer creating their own databases today, they using databases from companies. Data has been collected for commercial purposes. So if I gave my data to, you know, for a social network site or if I gave my credit card data for buying something on a site or I have joined a club or whatever, I gave those data for a specific purpose and I want to know if those data are than passed to the intelligence service or to the police. That I have the some right, that you know, my data are protected by the some standards and that is not he currently the case; […]" March 14, 2013 - Citizens & Consumers | ICT In 2012, the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. Commissioner Viviane REDING has separated the rules into a regulation, for general practice, and a directive**,** for law enforcement. Leading ICT journalist, Jennifer Baker, is joined by Sophie in't VELD MEP (ALDE)**,** to discuss the details of data protection reform in the EU.

[196] "Q: Let is talk about one of the big positive what we have seen recently, which it is the approval by the European Parliament (EP) of your proposal for a Data Protection Regulation (GDPR). Presumably, very happy about that connected fact? A: That was a landslide decision by the European Parliament (EP) and the EP by this decision shows it is capable to malls together in the interest of the citizens, in the interest of the economy, conflicting ideas, conflicting political views into one action to propose to the Council. Well done Parliament!" Aos 00':28". Leading ICT journalist Jennifer BAKER is joined by Viviane REDING, European Commissioner for Justice, Fundamental Rights & Citizenship, to discuss data protection regulation and the EU-US Safe Harbor agreement. Em http://www.vieuws.eu/ict/safe-harbor-reding-warns-us-that-progress-is-needed-before-summer/ a 26/mar./2014, Obtido a 25/abr./2014.

[197] "On 12 March 2014, the European Parliament adopted the text prepared by the Committee for Civil Liberties, Justice and Home Affairs (LIBE) which handles the Regulation in the European Parliament. LIBE rapporteur for the Regulation is MEP Jan Philipp Albrecht, and MEPs Dimitrios DROUTSAS, Axel VOSS, Alexander ALVARO, Timothy KIRKHOPE, and Cornelia ERNST serve as shadow rapporteurs."

EMs em relação à proposta *GDPR* que tem vindo a perder os seus anteriores aliados. As razões preconizadas, são várias: interesses divergentes entre os EMs por razões de políticas internas de captação e manutenção de investimento internacional na Indústria Digital e da Internet; «dificuldades da CE em responder a questões concretas e específicas por parte dos EMs no Conselho»; *timings* diferenciados entre os vários EMs, resultantes de opções políticas das próprias agendas nacionais, assim como, pressões internas de empresas da industria digital e de outras afins que anteveem dificuldades acrescidas na sua implementação e receiam os respetivos custos adicionais a eles inerentes; e, a principal de todas, a pressão dos *lobbies*[198] [199] –anti *GDPR*– de empresas multinacionais[200], na sua grande maioria americanas, que terão de despender muitos

[198] "So, from the perspective of an American observer, there one aspect to this conversation that as just been bizarre. We have a very inadequate Data Protection Regulation, but we have a very robust practices surrounding transparency, particularly, regarding the accessing of lobbyists to the Government and I have not heard[ed] discuss at all, except in assertive masterly in direction, that. It is curious for me this to see severed months ago was a front page column of the New-York Times, that have all the major Us Government relations, all offers with lobbying in terms of opening offices in Brussels? and that they were no obligations to disclosure their client list and the amount of money being been dispended in the lobbying and particularly for someone who is doing Data Protection issues. I cannot accept that the Commission is a 'black-box' and you do not know what is go in it and you know what is coming from out of it, which that been discussed and I relay, and left been clear after listening to this panel whether it is delayed to discuss that in public which case come as such and been playing right now and my apologies or whether non been discussed that in the context of the process that we have been but really seems to me that is something near to be said and I to ask to some of you to see to respond. Thank you." COHEN, Julie from Georgetown Law Center aos 01:08':35" 7th International Conference – 22, 23 and 24 January 2014, Brussels, Belgium - Computers, Privacy and Data Protection - Reforming Data Protection: The Global Perspective, CPDP 2014: EU Data Protection Reform: State Of Play, que pode ser obtida em https://www.youtube.com/watch?v=kl8an9Myrek; Consultada em 08/ago./2014.

[199] "Q: […] So, the final question. That, on the Data Protection Reform, on the lobbying, those been a lot of comments on the Civil Liberties Groups that: should we say, those some may interpret, on come from the way companies, particularly US companies and the US way of doing, or not doing, Data Privacy. Have you seen one of that or have you heard you colleagues breached? A: Of course, you know, in the end I have saw things that as a politician you have your own responsibility, and if you don't want give your own interpretation you don't. It is not difficult, ah! What I did not appreciate is that at the drafting stage, that is before the official legislative proposals were submitted to the European Parliament, the US Mission has been involved in drafting. That I do not appreciate, and I have pretty sure that my colleagues in US Congress, will not appreciate the EU civil Servants have been involved in drafting of US legislation before Congress, let's say, I don't think that is proper. Yes, let had been a lot of pressure but again that is for every member of the parliament (to), you know, to take their own position. I am very grateful that, let say, privacy activists and experts have intervened in the debate. Well, we need their expertise, we have listened them very careful and we will make that on our minds." March 14, 2013 - Citizens & Consumers | ICT In 2012, the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. Commissioner Viviane REDING has separated the rules into a regulation, for general practice, and a directive, for law enforcement. Leading ICT journalist, Jennifer BAKER, is joined by Sophie in 't VELD MEP (ALDE), to discuss the details of data protection reform in the EU.

[200] "[…]. And those who are asking for more, they take a high responsibility on then selves because, they may contribute to failure, and those like the Privacy Officer of Google, who go out and say 'this Regulation is death', well, they have a policy agenda, they want it death, that is not scientific analysis, that is political propaganda!" […]" NEMITZ, Paul, Representante do DG JUSTICE aos aos 35':45" 7th

milhões para a implementação da *securty by design*[201] subjacente à *GDPR*. Pelos vistos, estas, nunca desistiram, e têm vindo a conseguir aliados na UE a todo o custo. O pior dos cenários poderá, mesmo, acontecer com a entrada em plenas funções do atual PE, se a resistência do Conselho continuar, e se a atual e nova CE-"Juncker", não conseguirem "suportar" o projeto –agora alterado pelas contribuições dos anteriores MPEs: retorno a uma posição inicial, em que a CE terá de submeter, de novo, este ou, tudo indica, um novo projeto ao PE, que se verá na "obrigação" de o submeter à consulta dos MPEs, compila-la, redigi-la e complementá-la com os seus próprios contributos internos no comité *LIBE* ou outro com as mesmas funções. Por fim, chegar a um consenso alargado no plenário para que seja novamente aprovado. Isto para voltar de novo a enviá-lo para a CE e, em seguida, esta o submeta a nova aprovação no Conselho. Isto poderá demorar dois ou três anos[202]. Quem fica a lucrar com este atraso, quando a atual Diretiva data de 1995 (95/46/EC[LRG0A] [183]) –«data da época, pré-Internet» (Comissária Viviene REDING na Conferência de Imprensa de apresentação da *GDPR*, aos 2':28" a 25 de janeiro de 2012, disponível no sítio web da CE, em http://ec.europa.eu/avservices/video/player.cfm?ref=82655&sitelang=en, consultado em 26 de agosto de 2014)– está desatualizada, face às tecnologias atuais, ao crescimento "exponencial" da Internet, à proliferação e sofisticação de técnicas de intrusão entretanto utilizadas? O cidadão europeu, de certeza, é que não. E a maioria das empresas de pequena e média dimensão (PME/*Small and Medium Enterprises–SME*),

---

International Conference – 22, 23 and 24 January 2014, Brussels, Belgium - Computers, Privacy and Data Protection - Reforming Data Protection: The Global Perspective, CPDP 2014: EU Data Protection Reform: State Of Play, que pode ser obtida em https://www.youtube.com/watch?v=kl8an9Myrek; Consultada em 08/ago./2014.

[201] "Security by Design: The starting gun for a new 'crypto arms race' was fired by Edward SNOWDEN. His disclosures triggered a frenzy of activity to design new products and services that are NSA proof. […]" (MASCOLO & SCOTT, 2013, p. 13) e "Hello. I am from the Danish consumer council NGO and then in Denmark is that could be a problem here concerning the discussion in the Regulation/Directive, because the Government in Denmark that even know they like privacy and sure when comes to the opinion that they think the early day light and they want to support this debate and the public authorities and they think that as much effort from them to do the privacy assessment that is too expensive to working with 'privacy by design', so even know that, consumer NGOs and the industry are together to support the Regulation, the Government and maybe other (and DPAs, I do not know), but the Government is against the Regulation. […]" Idem.

[202] The worst scenario that I have is that the Council will not reach an agreement, has not reach in the last few months and the death lock will continue also until the end of the Summer, Which for the parliamentarians will mean, 'well we should rethink what we did in the previous time.' So it is mean, let is last open all the discussion again and have the 4000 amendments on the table and try to work on it again, which mean, we will not have the new prime work by 2020, probably. So these are the two scenarios I can draw and unfortunately, I have to say that once, we are not sigh the last allies of the Reform, the second scenario is more and more possible." Wojciech WIEWIÓROWSKI (WW), GIODO (PL), Polish Data Protection Authority (DPA) aos 26':30" Idem.

da Industria Digital e Internet europeia? Parece-nos, também, que não. É necessário que sejam tiradas as devidas elações políticas de todo este processo[203]. Mais uma vez, parece-nos que o "individualismo" de determinados EMs (*UK e D*[204]) se tem vindo a sobrepor ao bem comum da Comunidade na UE, neste caso relativamente aos Direitos dos cidadãos – a saudável utilização do Ciberespaço e da Cibersegurança na UE em detrimento de outros interesses. Felizmente, poderá existir ainda bom senso e aproveitar todo o trabalho feito até agora. Um indicativo, é o amplo consenso do desenquadramento da Diretiva atual –95/46/EC[LRG0A]– e a imperiosa necessidade de crescimento económico, assim como, a urgente diminuição do desemprego, em particular, dos jovens. Um imperativo que poderá permitir uma alternativa: a meta – definida pelo próprio Conselho– e consequente da Agenda Digital gizada pela CE –*DG CONNECT*, para entrada em vigor do futuro MDE em 2015. Este está indexado às metas definidas no *Europe 2020* e no programa *Horizon 2020*. Será, que se vai a tempo de se atingir um consenso político e adotar a nova *GDPR*, que como qualquer outra legislação «não é perfeita», mas que seria preferível à 95/46-EC[LRG0A], considerada por

[203] "Peter SCHAAR from the European Academy for Freedom Foundation and Data Protection in Berlin. Well, I completely agree with Paul NEMITZ assessment that we have a political question, but if I agree on this, we have to ask; 'what is the political question'. This is not limited to the substance we discuss. It is also a question of powers. It is a question of competences. And from my perspective much of the criticism against the approach of the Commission that is coming from Mss is against giving a way – competences – the legal field has well on the practical field that is now space for legislation in the MSs. The competence goes to the EP, the Commission and the Council. And therefore the [influence] opportunities to influence these procedures are weaker from the national point of view, than today. This is one aspect. And the second is: the role of the DPAs. The increase of the independence of the DPAs might seen as a threat by some Governments, because, if they are strong DPAs, –if they are real powers–, they are not dependent on the decisions of the Government and if they act in a different way, they might be the problem for the Governments. And I think, these are two crucial issues. On the first one, I think they could be a solution, at least if we focus on the main issues, in the Regulation, perhaps, they might be a third scenario, not only the both Wojciech WIEWIÓROWSKI[202] mentioned. Perhaps, the third scenario might be to focus on some main issues and to start again perhaps with these or to continue with these issues, not every single article or paragraph of the all Regulation – perhaps is necessary add the others. So we have to focus, but is not time to do this, today. I think, we try to support the EP and the Commission in been successful and we have try to convince our Governments, but if we fail, we have to avoid that will be a complete failure. So, but for the first scenario for me –scenario A– and we need a Regulation and perhaps, we have to consider – a scenario B–, after the election of the EP and after the Greek Presidency..[ ]" Senhor Peter SCHAAR ex-responsável pela Autoridade de Proteção de Dados da Alemanha aos 01:01':08" Idem.

[204] "[…]how much money this is going to cost them, you know, we know the United Kingdom (UK) ICO who is loosing founding as the new Regulation, so they has a big impact on how, for example, the UK has reacting.[…]" aos 22':21'e "[…]One issue that was not been mentioned in noun of this PW, you know, one of the biggest countries that is currently delayed, is actually, Germany, if far not mistaken. Perhaps, you know, It should be pointed out, to Germany that, you know, 82 million people that they data can easily keen out to a country where the DP Legislation is weaker, than it is in Germany, now, for example, Ireland. That could be a n incentive. So on balance, we would want the Regulation to pass speedily." À 01:07':16", Senhora Anne Felder, Privacy International (UK). Idem.

muitas entidades, manifestamente, obsoleta? Com uma vantagem: «a *GDPR* não é uma Diretiva, é uma Regulamentação de normalização, não tendo que ser transposta, embora traduzida e transcrita e aplicada de forma tácita a todos os EMs»[205], sendo igual para Irlandeses, Britânicos, Alemães, etc.. Logo se verá se isso é possível. Para os últimos desenvolvimentos, consultar, por exemplo o artigo *'European Union: European Union Law Update'* de 01 de setembro de 2014, redigido por O'SHEA, Robert e PAT English no sítio web http://www.mondaq.com/article.asp?articleid=337324&email_access=on , consultado a 02 de setembro de 2014.

O risco de "Securitização"206 nas Políticas de Cibersegurança

Com a situação atual de instabilidade internacional –resultante de fatores de ordem variada, problemas ancestrais, anteriores, não resolvidos e acima de tudo da disseminação vertical e horizontal do Poder– e o cenário de Multipolaridade ou mesmo Não-polaridade a médio prazo –segundo alguns autores[207]– será "normal" que as políticas relacionadas tendam, igualmente, a passar pelo processo de "securitização"[141] [208]. A tendência que se tem vindo a registar, de alguns anos para cá, do lado de lá do Atlântico, de preponderância da segurança nacional em contraposição aos Valores

[205] "[…].You know, I can only say, this Regulation 'will not be perfect', but will provide more instruments to the DPAs, will provide more instruments to individuals, it will ensure a 'higher coherence of application Law'. Who will not be perfection, but a highest coherence application of Law true the fact that is a Regulation, not a Directive - the Directive is initiated now, who always leads to diversion already across States, because MSs implements Directives differently […]" NEMITZ, Paul, Representante do DG JUSTICE aos aos 34':32" Idem.

[206] "One of the most important forms of "threat framing" is to categorise something as a "security policy" threat. In the research, this behaviour has come to be called "securitization." The opposite of such behaviour is, of course, to minimize the issue and avoid the negative connotations that threat images carry; that is, to undertake "desecuritization" (Buzan et al1998; Wæver 1995; Wagnsson 2000; Eriksson 2000). '*Setting the Agenda of Threats: An Explanatory Model*' *Johan Eriksson & Erik Noreen*, p. 11) www.pcr.uu.se/digitalAs**set**s/67/67519_3uprp_no_6.pdf; Consultado 29/jan./2013.

[207] "[...] Segundo as palavras de um antigo director de planeamento político do departamento de Estado: «A proliferação de informação é uma causa tão importante para a não polarização como o é a proliferação de armamento[*].» Ou tal como diz um analista britânico: «Enfrentamos cada vez mais riscos, ameaças e desafios que afetam as pessoas de um país, mas que têm origem maioritária, ou totalmente, nos outros países [...] crises financeiras, crime organizado, migração em massa, só para referir alguns [...] Uma das principais razões para essa dificuldade é o facto do poder se ter difundido tanto horizontalmente como verticalmente. Já não temos um mundo multipolar, mas sim um mundo não polar[**].»" (NYE Jr., O Futuro do Poder, 2012, p. 135) citando [*] Richard HAASS, «The Age of Nonpolarity», *Foreign Affairs* 87, n.º 3 (maio-junho de 2008): 47, e [**] Timothy GARTON-ASH, «As Threats Multiply and Power Fragments, the 2010s Cry Out for Realistic Idealism», *The Guardian*, publicado a 31/dez./2009.

[208] "Securitization: The EU used to have the goal to create a common 'area of freedom, security and justice'. However, at the face of new threats, the Commission and the member states tend to emphasize security over freedom, stressing the importance of introducing new security policy measures. In addition, private security companies have gained more and more influence in this field." (BENDIEK, "European Cyber Security Policy", 2012, p. 6)

Fundamentais e os Direitos Civis dos cidadãos, da privatização da segurança (BENDIEK, "European Cyber Security Policy", 2012, p. 6), etc., possa, também, se estender, de forma gradativa, à UE. Esta tendência tem-se vindo a denotar nos últimos anos na área da Segurança Interna da União em geral e na subárea da Cibesegurança, em particular, nomeadamente a seguir à delineação da estratégia do Programa de Estocolmo[209], «Em dezembro de 2009, o '*Stockholm Programme*'[210] foi aceite, o que representou um passo significativo na agenda de 'segurança interna' da UE.» (KLIMBURG & TIIRMMA-KLAAR, 2011, p. 30) No que diz respeito à Proteção dos Direitos dos Cidadãos, à Privacidade e à Proteção de Dados, as organizações cívicas, as ONGs, os Parlamentos nacionais e o Europeu terão, necessariamente, «uma palavra a dizer» e a sua quota-parte de responsabilidade –como "contrapeso"– em EMs democráticos e numa União que se quer "Modelo" de Valores e Direitos Fundamentais para terceiros países e outras Comunidades Regionais. Com a entrada em funções do atual PE e da nova CE presidida pelo Luxemburguês senhor Jean-Claude JUNCKER, resta-nos aguardar pela nomeação e assumir de funções –01 de novembro de 2014– dos novos Comissários responsáveis pelas áreas dos Assuntos Internos, Justiça, Direitos Civis, Agenda-Digital, Mercado Interno (ou designações equivalentes da nova orgânica da CE– "Juncker") e suas primeiras opções políticas e respetivas iniciativas legislativas e/ou de regulamentação, para verificarmos se a tendência se acentuará ou, se pelo contrário, o balanceamento entre os dois interesses contribuirá para um reforço interno dos Direitos e externo da projeção do ideal e dos Valores Europeus no Mundo, pois «a adoção de uma perspetiva de "securitização"[141] [208] não é a via mais apropriada para enveredar por um balanceamento de valores sociais que conduza à resiliência.» (TABANSKY, 2014, p. 9)

A projeção no Mundo dos Valores Fundamentais da União Europeia

Como consequência dos futuros "trabalhos de casa" e conclusão dos atuais (que se têm mostrado difíceis de alcançar), poderemos perceber se a UE –Instituições e EMs– pretende ser, mesmo, um exemplo em balanço de compromisso democrático

[209] "Concerning the general point of view, as the Stockhom Programme recognized, the EU security strategy tasks have to be clearly divided between the EU institutions and the MSs." (NOTO, 2013, p. 11)
[210] "See Council of the European Union, *The Stokchom Programme – An open and secure Europe serving and protecting the citizens*, 17024/09, 2 December 2009, http://register.consilium.europa.eu/pdf/en/09/st17/st17024.en09.pdf , consultado a 02/mar./2014.

entre a segurança interna –coletiva e individual– e a defesa dos Valores e Direitos Fundamentais, da Liberdade de expressão e de iniciativa dos seus cidadãos. Também, como resultado da atuação dos seus responsáveis políticos e instituições (a curto-médio prazo) conjuntamente com a Sociedade Civil, a Academia, o setor privado (através das *PPP*) –.e., dos *Stakeholders*– ficaremos a saber se a UE pretende ser um "Modelo" de governação regional –na área da Cibersegurança– que poderá ser adaptado a outras organizações regionais e/ou mundiais na administração deste tipo de problemáticas de Proteção de Valores Fundamentais, da Privacidade e da Proteção de Dados, etc., não comprometendo a [Ciber]Segurança dos seus cidadãos e dos EMs.

1.6 A União Europeia: Um Ciberespaço Aberto, Seguro e Protegido

> "Trust and confidence should be improved not only between states but also between the private and public sector. Through the strategy we are launching today sets out a number of priorities to improve IT systems, reduce cybercrime and establish an international cyberspace policy for the European Union (EU). This means looking at how Member States can work better together and what the EU institutions and agencies can do to help them. It means improving cooperation between different EU policy areas and promoting coordination between military and civilian sides. And It means that close work closely work with international partners, private sector and civil society." VP/HR ASTHON, Catherine in charge for Comum Security and Defence Policy (CSDP) on Press Conference about União Europeia Cybersecurity Strategy in Brussels - 07/fev./2013, texto consultado a 07/mar./2014 em http://europa.eu/rapid/press-release_SPEECH-13-108_en.htm e vista a 07/abr./2014 em http://ec.europa.eu/avservices/video/player.cfm?ref=I076087

> "We need to protect our networks and our systems and make them resilient. And that can only happen when all actors play their part and take their responsibilities. Cyber threats are not confined to national borders nor the cyber security be. So, our strategy so accompany by a proposal. Directive to strengthen cyber resilience within our single market. It will ensure that companies take measures needed for safe and stable networks." Vice-President KROES, Neelie in charge for the Digital Agenda on Press Conference about União Europeia Cybersecurity Strategy in Brussels - 07/02/2013, em http://ec.europa.eu/avservices/video/player.cfm?ref=I076087 vista a 07/mar./2014

O documento da UE-ECS é uma «magna carta» composta de frases políticas fundadas em princípios de boas intenções - na sua grande maioria, almejando aplicabilidade interna da UE – e um conjunto de boas práticas para o exterior. As intenções abrangem: a Segurança interna (de forma indireta), e direta para o Ciberespaço (em particular, o da UE); a dinamização da Economia Digital e das indústrias relacionadas (*DSM*) –de *software* e suas aplicações transversais à Sociedade Europeia, de segurança e, também, de defesa; a diminuição do desemprego,

particularmente dos jovens e no sexo feminino, e da infoexclusão das camadas menos jovens; a propagação dos Valores Fundamentais e a suposta afirmação da UE como ator internacional no Ciberespaço e na *IG.* As opiniões sobre o seu real potencial variam, entre os que nela participaram e acreditam e os restantes atores. Os próximos desenvolvimentos políticos resultantes da UE-ECS –a estratégia política da nova CE- "Juncker", «dos indigitados três comissários, *VP-Digital Single Market (DSM),* Andrus ANSIP (ex-Primeiro Ministro da EE, e ex-responsável por assuntos económicos, incluindo o Ciberespaço –políticas e economia Digital) , o *VP-Jobs, growth, investment and competitivness,* Jyrki KATAINEN e o Comissário para a *Digital Economy and Society* Günther OETTINGER»[211] (Comissária Nelie KROES aos 03':45") –e a sua articulação quer com a operacionalidade das ações constantes na Agenda Digital–, quer ainda, com a Diretiva RSI recentemente aprovada –a 13 de março de 2014.

As intenções da *CE,* com toda a certeza, foram as melhores. Definir cinco Princípios Gerais de atuação e, de igual forma, cinco Prioridades Estratégicas. Definir Ações –ou vetores específicos, dentro de cada Prioridade– que possam balizar, agora, ao atribuir responsabilidades e «guiar», depois, os responsáveis pelas ações setoriais. Mas, acima de tudo, que possam permitir as bases para –saber quem faz o quê– e a respetiva monitorização. Se possível, obter dados mensuráveis dos atores, para efeitos de eficiência da execução dos vetores das Ações e a eficácia em relação aos objetivos traçados nas Prioridades que foram definidas com base nos Princípios Geral da UE-ECS.

Para alguns, nomeadamente, membros do PE e para outros atores da Sociedade Civil e das ONGs, a UE-ECS é uma «amálgama» que vai desde «a persecução,

[211] "In an exclusive interview with viEUws, Neelie KROES - European Commissioner for Digital Agenda - discusses the biggest challenges facing her successors with Jennifer BAKER. Commission President Jean-Claude JUNCKER created two new positions to replace the current European Commissioner for Digital Agenda. If the European Parliament gives its green light, former Estonian Prime Minister Andrus ANSIP will become European Commission Vice-President for the Digital Single Market and Günther OETTINGER the Commissioner for Digital Economy and Society. KROES acknowledges that this new structure – in which two men will have to do one woman's job – will be challenging, but she supports the idea that more importance will be given to dialogue in the decision making process. Commissioner KROES identifies several fields that should be given special attention by the new Commissioners: cyber security, copyright, supporting the development of start-ups, fostering jobs and getting more women on boards. She underlines that including copyright in the portfolio of the Commissioner for Digital Economy and Society is a very positive move: 'excellent that copyright is back in the hands where solutions can be well prepared'." em http://www.vieuws.eu/ict/commissioner-kroes-to-her-successors-its-about-a-different-mindset/ . Consultada a 19/set./2014.

desnecessária na Estratégia (porque, para isso existem procedimentos judiciais), com *downloads* ilegais, num extremo, a problemas relacionados com a Segurança Nacional (interna), no outro, e de tudo um pouco, mas nada de substancial, no meio.»[79] Para estes críticos, a Estratégia «demorou demasiado tempo a ser produzida para o resultado alcançado, que ficou aquém das expetativas.» Não passou da necessidade de "redigir uma estratégia" de "boas intenções" e «meteu tudo no mesmo saco», o que, segundo os mesmos, «em democracia, não é, nem correto, nem saudável.»[79] Este conjunto de problemas com a UE-ECS, poderão, e até deverão, ser vistos sob a ótica de críticas da Sociedade Civil, das ONG e da Academia europeias, relacionadas com outras estratégias de UE a montante, onde se chega mesmo a afirmar que a UE "desaprendeu" em como construir uma Estratégia[148], e que a UE necessita de uma "Grande Estratégia" (BISCOP. Sven, '*EU Grand Strategy: Optimism is Mandatory*' N.º 36, July 2012, em www.egmontistitute.be , Security Policy Brief) e de renovadas/complementadas –e permanentemente monitorizadas– Estratégias Setoriais, incluindo uma nova UE-ECS.

Para a CE e os apoiantes, incondicionais, da UE-ECS, trata-se de um documento fundamental e abrangente. Dota a UE de um instrumento de trabalho válido, onde são definidas as políticas e os objetivos para o Ciberespaço, relacionados com outras áreas de interesse estratégico para a Europa e para o Mundo. Em termos de Princípios Gerais, de Prioridades e Ações, o instrumento –fundamental– foi criado, permanecendo disponível para trabalho dos atores responsáveis e interessados em assuntos relacionados com a Cibersegurança e o Ciberespaço – dentro e fora da UE. Como toda a Estratégia, a UE-ECS não será, necessariamente, perfeita nem está acabada ou "cristalizada", devendo adaptar-se a novas circunstâncias políticas e realidades internas e externas, sempre que for preciso "à luz" de novos dados e pela ação dos atores da UE.

Se compararmos a ECS da UE com a Estratégia para o Ciberespaço, por exemplo, dos EUA[33] (THE WHITE HOUSE, 2011), ela não é tão desenvolvida nem minuciosa, embora os princípios e intenções sejam semelhantes, com a diferença da UE-ECS não chegar ao ponto de abordar, com preocupação, assuntos relacionados com a Segurança Nacional e as intenções consequentes, resultantes de ações contra a mesma. A UE não está, de todo, neste momento e nem num futuro próximo, em condições de afirmar –intenções consequentes– relacionadas com ações contra a Segurança e Defesa da UE –ainda que no Ciberespaço– pela imersão na atual crise conjunta, por debilidade

de suporte na área da PESC e tibieza da PCSD. No que a este trabalho interessa, em particular, e como consequência da UE-ECS, foram definidos no último conselho Europeu, de 19 e 20 de dezembro de 2013, princípios e alguns objetivos a reter e a acompanhar a curto-médio prazo, relacionados com as PESC e PCSD (ver pp 27-28). Estes objetivos poderão vir a ter aplicabilidades práticas, muito importantes, na dinamização da indústria Digital, de Segurança e, mesmo, de Defesa na UE. Poderão, também, ter consequências nas implementações de políticas relacionadas com o Serviço Europeu de Ação Externa[212]num futuro próximo, nomeadamente, como suporte às PESC e PCSD, de preferência com apoio de cooperações a implementar –ou já acordadas– com outras organizações internacionais, como, a Organização para a Segurança e Cooperação na Europa[213] (OSCE/*Organization for Security and Co-operation in Europe–OSCE),* a OTAN e a ONU.

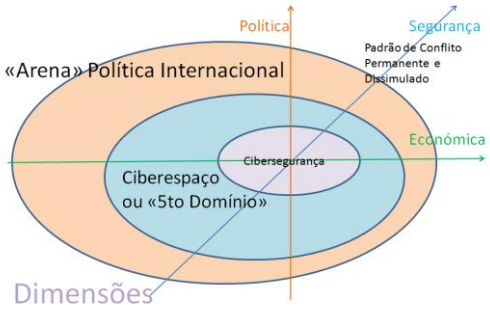

Ilustração 10- Diagrama –do autor baseado em (CALDAS & FREIRE, 2013)– das Dimensões das Políticas de Cibersegurança na "Arena" Internacional.

[212] "A Capacity building is one of the areas which is a possible that the biggest priority for the European External Action Service (EEAS), because the development aids are our traditional niche, we have here marked some funnies for the next 5 years for the project and we are going to find the model that works for us in the EU and of course we should coordinate that s globally, whit our partners." (TIIRMAA-KLAAR, 2013, pp. 3-13'10")

[213] "The second very important part to make cyberspace more stable, is to have a good international cyber policy. In Cyberspace what we have seen in the last decades is still a, it is a "baby policy", is what I called that! It is not comparable event to the traditional international is very known what to do. We have some such agreements within the Governments, we have the clear understanding of the behavior of the biggest actors. In cyber we just are doing the first steps and so, it is good very clear news that yesterday night, actually, there was a very important set of cyber norms agreed at the OSCE, which stands for the Organisation for Security and Cooperation on Europe, on that is exactly the countries are supposed to be doing in Cyberspace. So, we have the first set of cyber norms now agreed by almost fifty countries and participating states and stakeholders, so instead. So, I think this is very pretty achievement and I regale that this happen, this going to be a very good model globally, because the OSCE as, you know, as a large number of countries, that will be taken by other important security regional organizations, like ASEAN regional forum, where China also is part, so and this is a big with for the diplomatic community internationally that we have the first set for cyber norms now agreed." (TIIRMAA-KLAAR, 2013, pp. 2-08'13")

Capítulo II - Áreas de cooperação: União Europeia -OTAN

> "Common Security and Defence Policy (CSDP) - 37. In the framework of the CSDP, HIGHLIGHTS: the urgent need to implement and take forward the CSDP related cyber defence aspects of the Strategy to develop a cyber defence framework, as appropriate, and define concrete steps in this regard, also view of the European Council debate on security and defence foreseen in December 2013. A single point of contact should be designed within the EEAS to steer these efforts, […] the need to pursue and strengthen EU-NATO cooperation on cyber defence, identifying priorities for continued EU-NATO cyber defence cooperation within the existing framework, including reciprocal participation in cyber defence exercises and training, embedding cyber defence aspects in wider cyberspace policy." (Council of the European Union, 2013, pp. 6-7)

> "Governments need to focus on fighting the economic crisis and defence spending cannot be immune as they try to balance their budgets. However, the security challenges of the 21st century – terrorism, proliferation, piracy, cyber warfare, unstable states – will not go away as we focus on fixing our economies. While it is true that there is a price to pay for security, the cost of insecurity can be much higher. […]. multinational solutions will be vital for minimizing our costs […]. Then, as soon as our economies improve, we should consider increasing our investment in defence so that we can close the gaps. […], we must not forget that our values matter, our institutions matter, our way of life matters – and defence matters too." (RASMUSSEN, 2013, p. 3)

> "The United States is ahead of Europe in discussing and integrating (military) cyber security into its foreign and security policies. For the US, the biggest challenges at the moment are: updating legal frameworks, creating cyber rules of engagement for the military, building cyber deterrence and clarifying the cyber security roles and responsibilities of government and private sector actors." (SALONIOUS-PASTERNAK & LIMMÉIL, 2012, pp. 1-2)

Os primórdios da Cibersegurança na OTAN

A primeira decisão de proteção dos sistemas de informação e comunicação da OTAN foi colocada na sua agenda política na Cimeira de Praga em 2002, como reflexo dos acontecimentos durante a guerra dos Balcãs (1999). «O que aconteceu à OTAN no

decorrer do conflito[214] no Kosovo não foi, severamente, crítico, mas um alerta de pânico: o seu sítio web foi atacado por *hackers* 'patrióticos' Sérvios, e os respetivos servidores de correio eletrónico ficaram inoperacionais. O sítio web ficou 'em baixo' vários dias, o que veio a constituir um episódio de embaraço da imagem pública da organização.» (CAVELTY M. D., Cyber-Allies : Strengths and weaknesses of NATO's cyberdefense posture, 2011, p. 12) Mais tarde, os líderes Aliados reiteraram a necessidade de ser providenciada proteção adicional para os respetivos sistemas de informação na Cimeira de Riga em 2006. Com as ocorrências importantes na EE (como na Seção **1.4** se referiu), em que «uma série de ataques significativos a instituições públicas privadas na EE[215] em abril e maio de 2007 levaram a OTAN a tomar medidas sérias em relação às suas Ciberdefesas».

> "The Estonian incident was important for NATO's cyberidentity in several ways. First, it clearly showed the limits of old-school strategic logic in the face of cyberattacks and also shaped the perception that Alliance lacked both coherent cyberdoctrine and comprehensive cyberstrategy. Second, the incident also changed the way NATO perceived its own role in cyberdefense matters. Before the incident, NATO had almost exclusively focused on the protection of their own networks - afterward, the need for extend cyberdefense for the Allies came into focus." (CAVELTY M. D., 2011)

Depois foi na Georgia (em julho de 2008), onde ficou demonstrado que os ciberataques tinham potencial, só por si, de se tornarem um componente a ter em conta em cenário de guerra convencional[216].

Com estas preocupações em mente, o Conceito Estratégico adotado na Cimeira de Lisboa em novembro de 2010 evidenciou a necessidade de acelerar esforços em Ciberdefesa e incumbiu o Conselho do Atlântico Norte (*North Atlantic Council*–NAC) de desenvolver uma nova política da OTAN em Ciberdefesa, a qual veio a ser adotada pelos Ministros da Defesa em 8 de junho de 2011. O respetivo plano de ação tem vindo

[214] *Em 1999,* "Operation 'Allied Force': 'The first Internet War'. Sustained use of full-spectrum. of information warfare components in combat. Numerous hacktivism incidents." *e o surgimento de* "'Melissa': Shut down Internet mail, clogged systems with infected e-mails." (CAVELTY M. D., "The militarisation of cyber security as a source of global tension", 2012, pp. 108-109)

[215] "[...] was the systematic cyber attack of Estonian networks in 2007. When Estonian authorities began removing a bronze statue of a WW II-era Soviet soldier from a park, a three-week of so-colled Distributed Denial of Service (DDoS) swamped various Estonian websites with tens of thousands of visits, disabling them by overcrowding the bandwidth for the servers running the sites." (CAVELTY M. D., Cyber-Allies : Strengths and weaknesses of NATO's cyberdefense posture, 2011, p. 12)

[216] "The development and use of destructive cyber tools that can threaten national Euro-Atlantic security and stability represent a strategic shift that has increased the urgency for a new NATO cyber defence policy in order to strengthen the cyber defences not only of NATO Headquarters and its related structures, but across the Alliance as a Whole." (NATO A- Z, p. 4)

a ser implementado. A subsequente cimeira de Chicago de 2012 reafirmou essa política, e a sua implementação prossegue a bom ritmo, como se pode verificar pelas palavras, retiradas do Relatório Anual de 2012, do senhor ex-Secretário Geral da OTAN, Anders RASMUNSSEN[217] (a 1 de outubro o senhor Jens STOLENBERG –também da Noruega– entrou em funções), e como pode ser observado pela calendarização seguinte:

	j	*f*	*m*	*a*	*m*	*j*	*j*	*a*	*s*	*o*	*n*	*d*	*Obs.*
2010											Cimeira de Lisboa - Conceito Estratégico		Acreditação do CCD CoE em 2008 em Tallinn, Estónia
2011			Novo conceito de Ciberdefesa			Ministros da Defesa - Política de CiberSegurança e o Plano de Ação genérico - Aprovado				Implementação do Plano de Ação detalhado	Primeiro exercício Cyber Coalition		
2012		Euro contracto para a NCIRC de 58 Mé entre a NC3 A e o consórcio*			Cimeira Chicago - Reiterado o	Criação do NCIA (Intergação de seis agências OTANrelacionadas com as TICs)[218]	Estabelecido o NCIA				Criação do CTAC que depende do NCIRC CC	Implementação dos RRTs e segundo exercício Cyber Coalition	* Northrop Grumman e Finmecannica UK
2013										*FOC do NCIRC TC dependente do NCIRC CC que depende do CDMB - delayed*	Terceiro exercício Cyber Coalition		Uma vez ativado os RRTs respondem em 24h após o incidente [219]
2014		NAC alt. Defence Policy & Panning Committe p/ Cyber Defence C.		FOC do NCIRC Technical Center	DefenceMinisters : new Cyber Defence Policy				Cardiff Summit*				*Declaração da Cimeira de Gales, parágrafos 72 e 73 [220]

Tabela 2 – Calendarização –compilada pelo autor– da *Multinational Cyber Defence Capability* da OTAN

Para se perceber melhor as dependências entre as várias entidades inscritas no cronograma insere-se de seguida uma ilustração retirada do folheto *MN CD2 'Multinational Cyber Defence Capability Development Initiative'* da *NATO* C3 Agency.

[217] "NATO has continued to implement its new cyber defence policy though a comprehensive and ambitious action plan launched in October 2011. In the spring of 2012, NATO concluded an important contract for 58 million Euros with a consortium of private companies to significantly upgrade its unique operational cyber defence capability, the NATO Computer Incident Response Capability (NCIRC). When this project is completed in the autumn of 2013 and all NATO networks are brought under centralised protection, NATO's ability to defend its military and civilian networks against all types of intrusion and attack will be greatly enhanced[…]." (RASMUSSEN, 2013, p. 17)

[218] "También esse año, en julio, se creó la NCIA (NATO Communications and Information Agency), en la que se integran las seis agencias existentes relacionadas com las tecnologias de la información y telecomunicationes." Ver La Ciberdefensa en la Cumbre de Gales de La OTAN", NORÁN, David Ramirez, do Intituto Español de Estudos Estratégicos, n.º 13/2014, de 15/oct/2014, em www.ieee.es/Galerias/fichero/docs_informativos/2014/DIEEEI13-2014_Ciberseguridad_CumbreGales_DRM.pdf; consultado a 15/out./2014.

[219] Ver *Ciberdefensa. Equipos de Respuesta Inmediata de la OTAN* (BEJARANO, 2012)

[220] Wales Summit Declaration http://www.nato.int/cps/en/natohq/official_texts_112964.htm ; Consultado em 16/out/2014. (ver Anexo A.v)

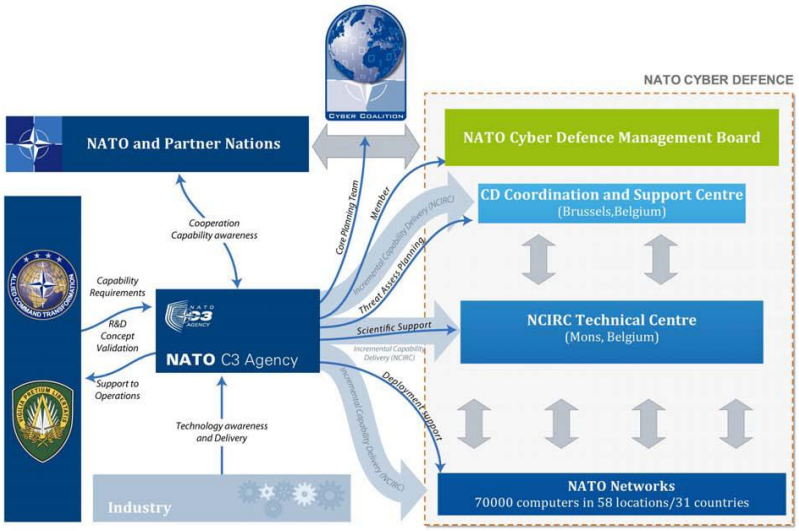

Ilustração 11- O papel da Consulting, Control &Command Agency na Ciberdefesa da OTAN

A '*NATO Consulting, Control and Command Agency'–NC3A*, através do seu do respetivo *Board*, constitui o corpo principal de consultadoria em aspetos técnicos e de implementação em relação à Ciberdefesa e ligação ao '*NATO Industry Assessement Group'–NIAG*. A '*NATO Military Authorities'–NMA* e a '*NATO Communication and Information Agency'–NCI* ficou responsável «por identificar os requisitos operacionais, a aquisição, a implementação e a operação das capacidades de Ciberdefesa da OTAN.» Esta última Agência (*NCI*), através do '***Threat Assessment Planning'*** pertencente ao '*NATO Computer Incident Response Capability*'[221]–***NCIRC,*** «comandado pelo***Cyber Defense Coordination and Support Centre–CDCSC***» (LAASME, 2012, p. 19) de Bruxelas e '***NCIRC Technical Centre'*** de Mons, na Bélgica (Ver Anexo A.v). Este último, «é o responsável pela provisão de recursos técnicos e operacionais no domínio dos serviços de Cibersegurança para toda a estrutura OTAN».

[221] "NCIRC is a two-tier functional capability where the NCIRC Technical Centre constitutes NATO's principal technical and operational capability and has a key role in responding to any cyber aggression against the Alliance. It provides a means for handling and repotting incidents and dissemination important incident-related information to system/security management and users. It also concentrates incident handling into one centralised and coordinated effort, thereby eliminating duplication of effort. Fist tier of NCIRC is the NCIRC Coordination Centre, located in NATO HQ with co-located staff from NATO HQ C3S. NCIRC Coordination Centre is a staff element responsible for coordination of cyber defence capabilities within NATO and with Nations, staff support to CDMB, planning of Annual Cyber Coalition Exercise and cyber liaison with International Organizations such as EU, OSCE and UN/ITU. Cyber Threat Assessment Cell (CTAC) is also co-located with NCIRC Coordination Centre." (NATO A- Z, p. 6)

Os Conceitos de Experimentação e sua a Conceção de Desenvolvimento

Esta implementação da OTAN é alicerçada nos conceitos de *Multinational Experimentation*[222]*–MNE*, atualmente na versão 7[223], e na sua «ferramenta» ou *Framework* metodológica do *Concept Development and Experimentation*[224]*–CDE* ou *CD&E*. Ambos, os conceitos, têm raízes na chamada «transformação militar EUA-OTAN». A filosofia subjacente é a de que «o sucesso é resultado, não só de recursos e meios militares eficientes, mas coordenados e suportados por iniciativas políticas e instrumentos económicos civis do poder[225] das nações aliadas.» (AALTOLA, SIPILÄ, & VUORISALO, 2011, p. 31)

No entanto, a ciberestratégia da OTAN [226], porque ambiciosa, também está sujeita a riscos de não ser, verdadeiramente, eficiente em toda a sua amplitude ou até

[222] "Multinational Experimentation (MNE) is a US Joint Forces Command-led (JFCOM) process which aims to create/discover crisis management capabilities to alleviate force transformation pressures that arise from operational threats with CD&E. Moreover, it aims to create crisis management knowledge, and crisis management processes, that is, perceived best practices. Subsequently, it distributes these creations amongst participants and beyond. Participation in this 'community of interest' is voluntary amongst coalition-friendly states." (AALTOLA, SIPILÄ, & VUORISALO, 2011, p. 35)

[223] "The next cycle, MNE7, began in January 2011 with the theme of 'Access to the Global Commons'." Idem (p. 37)

[224] "The purpose of Concept Development and Experimentation (CD&E) is to serve as a tool for the aforementioned transformation process. The most important function of this tool is to provide the intellectual association for future capabilities. CD&E is rapidly gaining relevance in many military structures, [...] As a transformational tool, CD&E functions primarily by providing fillers for capability gaps, thereby supporting capability development. Capability development covers strategic analysis, identification of capability requirements, solution identification and solution implementation.. CD&E is particularly instrumental when innovative answers to capability gaps are required. CD&E primarily develops conceptual solutions for capability shortfalls which have already been identified by other processes. However, it can also contribute to capability development through the introduction of previously unknown capabilities. There is some debate over which of these two CD&E functions should be primary." Idem (p. 32)

[225] "*Compulsory power* refers to the *Dahlian* definition of direct control over another; *Institutional power* refers to the ability to control socially distant others through rules and procedures constituting an institution; *Structural power* refers to the direct and mutual constitution of the capacities of actors; and *Productive Power* refers to the continuous and agile production of actor ness through often diffuse and *ad-hoc* social relations. is the least known. Yet, it seems to be particularly pertinent to the cyberspace domain which Nye defines as tending to flatten and diffuse power. Whereas structures produce hierarchical superiority and subordination among actors, productive power stems from much more tactic, diffuse, and situational Knowledge formations. These formations are often *ad hoc*, spontaneous, and fleeting in ways that cannot be captures by formal institutions or structures. Productive power requires situational awareness over the rapidly changing scenarios. Strict adherence to static institutional settings and structural formations is anathema to this kind of power." Idem (pp. 13-14)

[226] " [...] considers that: 'Adversaries will take the initiative and exploit Alliance vulnerabilities in both the virtual and physical domains of the global commons, including the realms of sea, air, space, and cyberspace.' Access to, and 'unfettered use' of the commons must be ensured. Access in particular is seen as 'pivotal to the success of all Alliance operations.' In other words, the flows of commerce, communications and information, military capability, and governance - indeed the functioning of the global (western, liberal-democratic) system - must be ensured. One step in achieving this its to ensure

contraproducente, aconselhando que «a OTAN deverá ter de começar a pensar em investir na gestão de espectativas,» como ressalvam alguns analistas, entre eles, Myriam Dunn CAVELTY do *CCS* do *ETH* de Zurique:

> "The problem is that two different types of security logics clash when an organization like NATO takes on cybersecurity or cyberdefense. When the words security and defense are used with the prefix 'Cyber,' they mean something fundamentally different from security and defense in an (inter-)national security setting. There, security is a binary concept: either one is secure or one is insecure. Cyberdefense on the other hand is a 'sexy' word for computer security or information assurance, which is concerned with analyzing the risk to information networks and then mitigating the identified risk by technical (and occasionally organizational) means. Risk is a concept aimed at managing an ongoing process, and is by definition linked to the notion of being insecure. As every systems administrator knows, his or her goal is not to eliminate all risks (even if this were possible) but to manage them in the most cost-effective way. Information networks, therefore, can never be 'secure' in the national security sense. In fact, the opposite is true: cyber incidents are deemed to happen under the logic of risk because they simply cannot be avoided." (CAVELTY M. D., Cyber-Allies : Strengths and weaknesses of NATO's cyberdefense posture, 2011, p. 15)

Devido a esse choque concetual, a OTAN, «para não vir a ficar desacreditada no domínio da opinião pública, deveria procurar desde já esclarecer que a sua ciberestratégia não será totalmente imune às consequências de ciberataques futuros perpetrados, em particular, contra as suas redes de comunicação e informação e dos Aliados em geral», pois como vimos, essa tarefa (apesar de todo o cuidado na sua definição, implementação, operacionalização e montantes envolvidos nessa «solução»), é complexa, e pelas razões apontadas, «não será 100% segura, porque na área do Ciberespaço o conceito de 'estar seguro' não é dicotómico», mas sim, gradativo.

No que concerne à necessidade de aproveitar sinergias entre as duas organizações UE-OTAN, como reflexo da situação económica, financeira e orçamental de que a grande maioria dos EMs de ambas as organizações atravessa, por um lado, e também devido ao substancial desenvolvimento que alguns dos membros da OTAN adquiriram, bilateral e multilateralmente, pela implementação da estratégia de Cibersegurança da organização, por outro, a UE teria vantagens acrescidas em apreender e, se possível, utilizar alguns dos ensinamentos e procedimentos *da* OTAN. O

safe access to the commons. Thus, MNE7 is focusing its attention on the interconnections of the system, rather than on the objects of the system. Building on the logic of past MNE cycles, 'flow-security' in MNE7 will be developing as a multinational inter-agency framework, as the sheer complexity of these tasks requires intensive orchestration and synchronization amongst different actors." Idem (pp. 37-38)

Conselho Europeu de dezembro p.p. registou orientações nesse mesmo sentido. Como atrás referido (ver p. 28), estas conclusões foram importantes, quer no tempo, quer na oportunidade. A indústria de Defesa Europeia –apesar de se encontrar numa fase difícil, devido aos cortes no investimento dos EMs de 10.000 milhões de Euros em cinco anos, detém ainda toda a sua capacidade de investigação e desenvolvimento[227]– necessita urgentemente de projetos para poder continuar a ser viável financeira e economicamente, em particular, podendo recorrer ao *Horizon 2020*. A oportunidade resulta deste ano entrar em funções a nova CE–"Juncker" e a nova VP-AR, italiana, senhora Federica MOGHERINI, que poderão dar um novo impulso no sentido da consolidação do SEAE na persecução dos objetivos da PESC em geral e da CSDP em particular, como instrumentos de projeção de *Softpower* da UE.

2.1 A procura de Quadros Jurídicos e Referenciais Reguladores

> "*Domestic and international legal frameworks must be modernized*. These provide both national and international limits and create certain expectations of behavior. States should aim to create international cyber rules of engagement concepts and guidelines, and potentially seek some limitations on the use of cyber arsenals against each other. Prospects for pre-emptive strikes must also be addressed. Such cooperation is necessary to avoid uncontrolled escalations and spirals of reprisals that shift impacts from the digital to the physical domains. This necessitates discussing how automated cyber counter-attacks can be. Discussions on legal frameworks also require extensive societal debate on the evolving balance between privacy and surveillance. States must cooperate globally to clarify and potentially seek some limitations on the use of cyber arsenals against each other." (SALONIOUS-PASTERNAK & LIMMÉIL, 2012, p. 7)

> "Currently, governance in the area of cyber security is characterised by a certain duality. As far as regulatory issues are concerned, the European approach is generally liberal, meaning that the private actors are encouraged to partiCIPate in the process. However, when it comes to questions of national security, there is a clear emphasis on the role of the state." (BENDIEK, "European Cyber Security Policy", 2012, p. 12)

No domínio do Ciberespaço, em geral, e da Internet, em particular, um dos maiores "quebra-cabeças" que se tem colocado, quer diretamente no plano técnico, quer de uma forma colateral, mas muito significativa no plano político institucional, é o chamado "problema da atribuição" (já anteriormente referido[125]) de um ciber-ataque. Isto, especialmente, quando estes atingem um determinado grau de sofisticação e/ou

[227] "[…] Europe's defence industry remains a high-performing industry and high-performing in terms of technology. […]" Ver aos 2´:40" a entrevista da Presidente-Executiva da ADE, senhora ARNOUD, Claude-France em https://www.youtube.com/watch?v=S10yyZwYVzo; consutaldo a 10/ago./2014.

uma amplitude tal, que não é possível dissimula-lo da opinião pública[228], muito em particular, quando os possíveis autores são outros Estados ou organizações –*proxies*[229]– que dependam direta, ou indiretamente, daqueles de forma operacional e sistémica.

A ausência de definições das ações e do rigor dos conceitos

A principal preocupação no que concerne a trabalho de análise e investigação no campo da Segurança –e mais concretamente no subcampo do Ciberespaço– resulta de dispersão nos conceitos e alguma inconsistência no rigor. Estes, induzem a que «nós temos de ser muito precisos, porque as palavras são importantes – em particular quando são usadas nas relações internacionais.» (SCHMIDT, 2011, p. 50) A profusão de definições, a sobreposição de algumas, –p.e. *CNE e CNA*, Ciberguerra e "Ciberhactivismo" ou Ciberespionagem (CAVELTY M. D., "Cyberwar: Concepts, Status quo, and limitations", 2010), «utilização de força *versus* ataque armado» (LOSEY, 2014), etc.– e justaposição indevida em domínios distintos, –p.e. Ciberdomínio e Ciberespaço[230], «*Global Common versus Common* incompleto»[26], etc. Isto deve-se, por um lado, a ser este subcampo de análise relativamente recente, onde ainda não houve tempo para suficiente "maturação" em relação às agendas políticas dos Governos[3] em geral e às disciplinas de Ciência Política e Relações Intencionais em particular (ver p. 43). Por outro lado, como "subcampo com temas interessantes e oportunos", ter atraído uma profusão de quadrantes –áreas de investigação e intervenção de instituições e indivíduos (analistas, investigadores, estudiosos, curiosos, media, etc.)– nele, interessados (ver Nota de rodapé 79, p. 22). Paulatinamente, este processo de depuração tem-se vindo a fazer por intervenção da Academia, da Sociedade Civil e das ONGs, etc. No entanto, o caminho será longo e por vezes indireto, porque, complexo:

[228] "[…] the shift from an open secret to a published secret is a game changer. It is a game changer because it exposes the gap between what governments will tolerate from one other under cover of darkness and what publics will tolerate from governments in the light of day […]" (MASCOLO & SCOTT, 2013, pp. 1-2)

[229] "[…] Otherwise, states´ cyber operations will increasingly push boundaries of the acceptable in order to tease out the limits of what can be gotten away with: states will resort to proxy combatants, digital camouflage and other acts of perfidy in order to circumvent constraints on armed conflict that were developed in a non-digital era." (MUELLER, 2014, p. 2)

[230] "Cyberspace arises out of the Internet[2], the global set of interlinked computer data networks that are used for both physical and ideational purposes.[*] The name 'cyberspace' is given to the digital data trail generated by interconnected computers. While cyberspace cannot be spatially located[24], it gives rise to 'real' effects. The contrast to other operational theaters is simple: cyberspace cannot be reduced to physical attributes only. It is partially a material domain, used for commercial activities (e.g. e-banking) and infrastructure management (e.g. industrial control systems), and partially in ideational domain – a platform for information exchange and communication." (MUELLER, 2014, p. 4)

Devido à intricada relação entre sociedade, tecnologia e política, com as duas primeiras cinéticas e voláteis e a última hierarquicamente mais rígida e pouco recetiva às mudanças que aquelas têm vindo a sugerir e mesmo, em alguns casos, a impor.

A incerteza de consequências de atividades de atores estatais e de *proxies*

Segundo alguns autores, no quadro atual de *status quo*, existem pressupostos indefinidos e "vazios" na aplicação de conceitos –i.e., *jus ad bellum*[231]– das normas internacionais e respetivas incongruências para o Ciberespaço. Por exemplo, a considerar um ciber ataque como um ataque armado ou simplesmente uma utilização de força, desde que esta ação não tenha consequências cinéticas. No entanto, poderá –na prática– uma utilização de força no ciberespaço ser mais gravosa para um estado do que um verdadeiro ataque armado, como é sugerido por estes dois exemplos:

> "(i) A state bombs the stock Exchange building of another state at night. There are no causalities. A physical back-up and business continuity plan are in place. Trading is not disrupted; (ii) A state launches a cyber attack against the stock Exchange of another state at night. There are no causalities. The back-up is also compromised electronically and the business continuity plan fails. Trading is disrupted for a week." (MUELLER, 2014, p. 7)

Apesar de no caso (ii) não ter havido ação cinética, as consequências para o Estado "vítima" do ataque acabam por ser muito maiores em termos de danos para a Economia do mesmo. No entanto, *a priori*, este caso se enquadra numa ação de força e não num ataque armado, e nem toda a ação de força deve constituir um ataque armado pelo Artigo 2 da Carta da ONU. No entanto, «e concetualmente, existem fortes razões para suspeitar que o ciberespaço deveria estar sujeito a um corpo legislativo próprio.» (MUELLER, 2014, p. 5) Ainda, segundo o mesmo autor: «1. A Comunidade de estados necessita comummente de chegar a acordo sobre normas padrão de legalidade que definam o que possa constituir um ataque armado ilegal no ciberespaço;» e «2. A Comunidade de estados necessita estabelecer uma obrigatoriedade de assistência mútua intrafronteira para investigações relacionadas com o Cibercrime.» idem (p. 2) Por outro

[231] "[…] is the title given to the branch of law that defines the legitimate reasons a state may engage in war and focuses on certain criteria that render a war just. The principal modern legal source of jus ad bellum derives from the Charter of the United Nations, which declares in Article 2: 'All members shall refrain in their international relations from the threat or the use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations'; and in Article 51: 'Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations.' Consultado em http://www.crimesofwar.org/a-z-guide/jus-ad-bellum-jus-in-bello/ a 15/ago./2014.

lado, alguns autores –de ambas as "margens" do Atlântico[233] [235]– são de opinião que, pelo menos por agora, as leis que existem e estão acordadas na Comunidade Internacional, como p.e., a Lei Humanitária Internacional LHI/*International Humanitarian Law–IHL*[232] *ou* Lei dos Conflitos Armados/*Law of Armed Conflict–LOAC*[233] no que concerne ao *jus in bello*[234] em relação a possíveis conflitos são extensíveis, de igual modo, ao quinto novo domínio do Ciberespaço[235].

Esta situação conduz-nos ainda ao nuclear "problema da atribuição"[125] no Ciberespaço, «o principal problema e no qual tem sido colocada a maior das preocupações em relação aos ataques perpetrados pela Internet.» (KNABE, 2010, p. 3) Apesar de poderem existir tecnicamente formas de atribuição, embora complexas e demoradas –por envolverem análise forense e devido à mutação vertiginosa das tecnologias e técnicas envolvidas[126]– não existem inequívocos mecanismos legais

---

[232] "There is no agreement on what to call *jus in bello* in everyday language. The International Committee of the Red Cross (ICRC) and many scholars, preferring to stress the positive, call it international humanitarian law (IHL) to emphasize their goal of mitigating the excesses of war and protecting civilians and other noncombatants. But military thinkers, backed by other scholars, emphasize that the laws of war are drawn directly from the customs and practices of war itself, and are intended to serve State armies. They commonly use the more traditional rubric, the laws and customs of armed conflict or more simply, the laws of war." Consultado em http://www.crimesofwar.org/a-z-guide/jus-ad-bellum-jus-in-bello/ a 15/ago./2014.

[233] "The official policy of the United states [por exemplo,] is that the Law of Armed Conflict (LOAC) applies to cyberspace, since all new technologies are subject to existing laws of war.* See KOH. Harold H. '*International Law in cyberspace.*' Harvard International Law Journal (2012) Vol. 54" (MUELLER, 2014, p. 7)

[234] "*Jus in bello*, by contrast, is the set of laws that come into effect once a war has begun. Its purpose is to regulate how wars are fought, without prejudice to the reasons of how or why they had begun. So a party engaged in a war that could easily be defined as unjust (for example, Iraq's aggressive invasion of Kuwait in 1990) would still have to adhere to certain rules during the prosecution of the war, as would the side committed to righting the initial injustice. This branch of law relies on customary law, based on recognized practices of war, as well as treaty laws (such as the Hague Regulations of 1899 and 1907), which set out the rules for conduct of hostilities. Other principal documents include the four Geneva Conventions of 1949, which protect war victims—the sick and wounded (First); the shipwrecked (Second); prisoners of war (Third); and civilians in the hands of an adverse party and, to a limited extent, all civilians in the territories of the countries in conflict (Fourth)—and the Additional Protocols of 1977, which define key terms such as combatants, contain detailed provisions to protect noncombatants, medical transports, and civil defense, and prohibit practices such as indiscriminate attack." Consultado em http://www.crimesofwar.org/a-z-guide/jus-ad-bellum-jus-in-bello/ a 15/ago./2014.

[235] "So, the second step that we need to do internationally is to make sure, is the «rule of law» and then the existing Laws, nor new Laws applying in Cyberspace. There are some calls for new treaties and new laws and sometimes in the biggest internationally organizations, and we «the cyber people» to think that new laws can fix Cyberspace. We have to apply the existing ones. We have the Budapest Convention for Cybercrime to address problems related to criminal activities in Cyberspace. We have the International Humanitarian Law [- IHL], that has set very long time ago. The principles of kindling of behavior of the States during in conflicts. So, this is just has to applying now to Cyberspace, because that really, do not matter how do I hit you. I need to follow the some moral principles right! So, then we have other international Laws, like human Right Laws and other status that apply in Cyberspace." (TIIRMAA-KLAAR, 2013)

internacionais de atribuição efetiva pela responsabilidade da ação de força, quando não há danos físicos[236]. O problema da atribuição complica-se quando os Estados –para camuflarem as suas ações– utilizam atores não estatais, grupos e/ou indivíduos[219] [237] – nacionais e/ou internacionais– para conduzirem ações hostis no ciberespaço contra outros indivíduos, grupos, organizações, empresas e/ou Estados da comunidade internacional. Ainda assim, segundo alguns autores será possível enquadrar os comportamentos de atores do tipo *proxy* –por parte de Estados e de atores não estatais [para mais informações, consultar o trabalho de (RATTRAY & HEALEY, 2011, p. 82) que são de opinião que «estes constituem uma ameaça tão importante como os atores estatais,» pertencente ao projeto do *Cyber Statescraft Initiative on The Atlantic Council*[125] (ver p. 48)]– em Artigos constantes do Relatório da ONU intitulado 'Responsabilidades do Estado' ou '*Draft Articles of State Responsability*' elaborado pela sua Comissão de Legislação Internacional[238] em 2001 (SCHMITT & VIHUL, 2014, p. 57).

Este problema da atribuição implica a jusante o tópico da retaliação. Sem um enquadramento legal internacional aceitável e comummente aceite não será possível distinguir –hoje– entre uma ação de força e de ciberespionagem, respetivamente, i.e., de preparação[84] de uma ação futura de ataque armado (GEERS, 2013). Segundo alguns autores, as ações de ciberespionagem deveriam destrinçar entre a «perpetrada com fins industriais e de roubo de propriedade intelectual que deveria ser enquadradada ao nível a Organização Internacional do Comércio (OIC/*World Trade Organization*–*WTO*)»

[236] "The clarity of the concept relied on by the Law of Armed Conflict is diluted in cyberspace. The LOAC restricts the use of military force between states: Article 2(4) of the United Nations Charter outlaws the use of force against the territorial integrity of another state, and Article 51 of the Charter entitles a target state to respond against an armed attack with its own, proportionate use of a force. US doctrine in the event of a cyber intrusion is to assess its physical effects.** **For a discussion of just such assessments are made, see SCHMITT, Michael N. (Ed.) '*Tallinn Manual on the International Law Applicable to Cyberspace*': Cambridge University Press, 2013." (MUELLER, 2014, p. 5)

[237] "But to further attenuate the difficulty of attribution, a variety of non-state actors operate in this environment. While some pursue independent agendas, other act in varying degrees of support for particular states and their policy objectives. In some cases, they act as proxies for the states concerned." (SCHMITT & VIHUL, 2014, p. 55)

[238] "U.N. International Law Commission, Report of the International Law Commission, Draft Articles of State Responsibility, U.N. GAOR, 53rd Sess., Supp. No. 10, U.N. Doc. A/56/10 (2001) [here-inafter Articles on State Resposability]. The general International law of State Responsibility has not been set forth in a treaty. Rather, it emerges as the product of State practice that is engaged in out of *opinion juris*, i.e. a sense of legal obligation (customary international law). The International Court of Justice has recognized customary law as a valid form of international law in the Statute of the International Court of Justice. Statute of the International Court of Justice art. 38(1)(b), June 26, 1945, 59 Stat. 1055, T.S. No. 993, 3 Bevans 1179."

(MUELLER, 2014, p. 9), da "normal" ciberespionagem entre Estados –prolongamento da tradicional espionagem de recolha de informações– que seria tolerada pelo "princípio" da reciprocidade (MASCOLO & SCOTT, 2013, p. 3) entre a comunidade internacional. Outro documento muito importante no contributo de enquadramento legal –mas não totalmente aceite pela Comunidade Internacional, porque foi elaborado pelo *CCD CoE* da OTAN– é o chamado Manual de Tallinn e que poderá ser consultado on-line em https://archive.org/details/TallinnManual. Acedido a 08/dez./2013.

2.2 Papéis e Responsabilidades das Parcerias Público-Privadas

> "***Public-Private Partnerships are compulsory in cybersecurity***. Governments and the private sector are jointly responsible for building sound cybersecurity within states. Protecting critical national infrastructures is an extremely important aspect of cybersecurity. Securing this critical infrastructure, which in most western countries is owned by private companies, should therefore be the first priority of national cybersecurity programmes. To facilitate this, mechanisms must be created through which society can benefit through the state from the best 'cyber wizards', who predominantly work for the private sector. These mechanisms should ensure assistance is available both in peacetime, as well as during emergencies and wartime[239]." (SALONIOUS-PASTERNAK & LIMMÉIL, 2012, p. 7)

> "For more than a decade[240], efforts have been underway to establish Public-Private Partnerships (PPP) for Critical Infrastructure Protection (CIP). Due to issues arising in connection with their implementation, there has been increasing criticism in recent years questioning the usefulness of such PPP. However, cooperation between the state

[239] "In Finland, a history of cooperation and legal provisions created for a large reservist military can form the basis of an initial solution. However, small countries such as Finland must also contend with the reality that they have relatively little to offer large multinational companies when discussing public-private partnerships. On a national level, however, even large multinational companies can be mandated to take specific precautions in support of national strategies, which include following minimum security standards and building resilience into daily business operations." (SALONIOUS-PASTERNAK & LIMMÉIL, 2012, p. 7)

[240] "Critical infrastructure protection (CIP) is currently seen as an essential part of national security in numerous countries around the world and a broad range of political and administrative initiatives and efforts is underway in the US, in Europe, and in other parts of the world in an attempt to better secure critical infrastructures[* **]. One of the key challenges for such protection efforts arises from the private sector since the 1980s and the globalization processes of the 1990s, which have put a large part of the critical infrastructure in the hands of private enterprise. This create a situation in which market forces alone are not sufficient to provide security in most of the CI 'sectors'[***]. At same time, the state is incapable of providing the public good of security on its own, since an overly intrusive market intervention is not a valid option either; the same infrastructures that the state aims to protect due to national security considerations are also the foundation of competitiveness and prosperity of a nation. Therefore, any policy for CIP must absorb the negative outcomes of liberalization, privatization, and globalization, without. *[1**, p. 527ff]. **E. BRUNNER, M. SUTER, the International CIIP Handbook 2008/2009 – An Inventory of Protection Policies in 25 Countries and 6 International Organizations, Center for Security Studies, Zurich, 2008.***.M. Dunn CAVELTY, K. S. KRISTIENSEN (Eds.), Securing the Homeland: Critical Infrastructure, Risk, and (In)Security, Routledge, London, 2008." (CAVELTY & SUTER, "Public-Private Partnership are no silver bullet: An expanded governance model for Critical Infrastructure Protection", 2009, pp. 1-2)

> and the private corporate sector in CIP is not only useful, but inevitable." (CAVELTY & SUTER, "Public-Private Partnership are no silver bullet: An expanded governance model for Critical Infrastructure Protection", 2009)
>
> "*Privatisation of governance*: Also the traditional distinction between the private sector and the public sector is increasingly fading in the emerging political structure [...]. Without the technological expertise of private companies, it is difficult to identify the relevant threats and response to them accordingly. Many private companies are also responsible for critical infrastructure in energy, health or transportation. Involving these companies in risk and crisis management as well as threat identification processes is a decisive part of maintaining public safety, which, on the other hand, has to be guaranteed by the institutions that have a constitutional right to do so." (BENDIEK, "European Cyber Security Policy", 2012, p. 6)

Como já vimos (no Capítulo I, pp. 41-42), uma porção substancial do Ciberespaço ou, se quisermos, grande parte da Internet é detida ou, pelo menos, concessionada a entidades privadas. Para este tipo de entidades, a primeira prioridade é o lucro, que permita o retorno do investimento no mais curto intervalo de «orientação ao projeto, à eficácia e à continuidade de negócio.» No que concerne às preocupações do Estado, em particular, as ICs, por serem vitais para o funcionamento da sociedade, há «uma orientação a um programa e à segurança coletiva.» Esta é uma componente imprescindível que, muitas vezes, não entra no modelo de negócio de entidades privadas, até que uma de três situações o exijam: necessidade intrínseca do conceito de segurança ao próprio modelo de negócio em situações muito peculiares; uma imposição extrínseca do conceito por parte do Estado ou do supervisor, ou; a demonstração cabal que a introdução do conceito no modelo, apesar de ter custos, resulta em uma mais-valia para o negócio. Como se pode induzir destes considerandos, raramente o conceito de segurança coletiva –que deve ser assegurada pelo Estado[241]– detém "peso" necessário para que aquela faça parte da equação de uma PPP que é responsável por uma IC na "obrigação" de contratualização de exploração. Isto é, haverá uma disjunção entre a teoria e a prática. Este desfasamento poderá ser colmatado de várias formas: coercivamente, co-optativamente ou induzindo-o na forma "engenhosa" de pertença "genuína" em reduzidas associações de ***Stakeholders*** «com verdadeiros interesses em comum, colaboração e confiança recíproca.[242]»

[241] "[…] Generating security for citizens is a core task of the state: therefore it is extremely delicate matter for the government to pass on its responsibility in this area to the private sector." Idem (p. 3)
[242] "The fundamental problem is that trust can only be developed through collaboration, which in turn also depends on trust." Idem (p. 4)

Modelos de Governação mais dinâmicos e funcionais

O principal problema subjacente ao paradoxo das PPPs e das PICIs é o da «partilha de informação» relativa a incidentes de segurança. Existem três eixos de partilha: a horizontal que permite o fluxo de informação entre os privados da mesma ou de várias associações e o Estado; a vertical, que facilita o fluxo na "cadeia de produção"[30] de cada entidade específica –privados e Estado–, a montante e a jusante; e, por fim a internacional, pois grande parte destes privados, são multinacionais. Qualquer uma das três incorpora um risco sério de "fuga de informação" confidencial e/ou estratégica. Estes receios não permitem, na prática, o estabelecimento de condições de entendimento e confiança plenas entre os vários atores das PPPs, a menos que estas sejam de dimensão reduzida, com uma filosofia do tipo *win-win*, em que o Estado seja visto como um "verdadeiro" parceiro e não um agente que impõe normas e regulamentos. Os receios, também, existem quanto ao armazenamento e tratamento da informação estratégica e/ou confidencial –pelo Estado– de forma que a «relação de confiança» possa ser mantida.

Atendendo às razões atrás descritas "da cinética" da tecnologia, da volatilidade dos fluxos de informação, da vulnerabilidade do Ciberespaço e da hierarquia e rigidez das entidades políticas e supervisoras do Estado e de Governação, será necessário encontrar um novo modelo de articulada gestão das PPPs –ou outra designação mais apropriada– nas PICs em geral e nas PICIs em particular. Vários autores têm trabalhado em novas abordagens ao problema baseando-se na Teoria da Governação ou de "Governança" ou *Governance Theory* aplicada a estruturas em rede –que é o caso das PICIs no Ciberespaço. Eles preconizam um modelo de «Meta-governação» e uma nova função para o Estado: o de catalisador de soluções. Segundo este modelo, o Estado deixaria de ser o "dono" e supervisor das parceiras existentes –modeladas de forma hierárquica– e passaria a ser um elemento ao nível dos restantes, delegando competências: «*downwards* (localização); *upwards* (supranacionalização); ou *sideways* (privatizando-as).» Poderia, sugerir soluções de *downsizing* se necessário –das existentes e que encontrem dificuldade de funcionamento atual– ou até mesmo criando condições para o aparecimento de novas, se for o caso, tornando a gestão mais flexível e natural possível. Isso facilitava a cooperação, o entendimento e a confiança entre os atores envolvidos de forma voluntária nas parceiras "em rede" de gestão das PICIs, e

nos respetivos fluxos de informação daí resultantes, esbatendo as dificuldades e desconfianças, melhorando a sua dinâmica interna, a partilha de riscos e o resultado global de funcionamento também em prol da segurança coletiva, uma vez que é no setor privado das economias ocidentais –devido à sua excessiva exposição– que se encontram os recursos humanos e financeiros com maiores aptidões para a pesquisa e implementações necessárias[116] aos atuais e novos desafios –dinâmicos e de solução complexa– do Ciberespaço.

2.3 As Regras de Conduta para Ações Militares no Ciberespaço

> "[…]. The term cyber war covers attempts of a state to harm another state by attacking it via the internet. However, all of these working definitions remain ambiguous**. There are, furthermore, no clearly defined political and legal boundaries for differentiating between cybercrime, cyber espionage and cyber war, which makes classification all the more difficult[243]." (BENDIEK, "European Cyber Security Policy", 2012)

Devido à permissividade do Ciberespaço (atrás referida), ausência de separação perfeitamente definida entre o que pertence à jurisdição militar e civil na Internet, a mesma é partilhada por entidades e organizações de ambas as naturezas –criando "zonas híbridas" operacionais. Surgem dúvidas de como proteger as infraestruturas de suporte ao processamento, armazenamento e comunicações de possíveis ataques, ainda que virtuais, quando estas poderão ser consideradas como alvos "militares" (devido à utilização da Internet, no mínimo, p.e., para logística das operações), mas sendo pertença de empresas ou organizações civis e algumas, mesmo, multinacionais, ou concessionadas e geridas por entidades privadas. Este problema, sendo global, revela-se mais crítico nos países "ocidentais" com economias de mercado, uma vez que, em países onde a economia é "controlada" ou subvencionada pelo Estado, este terá, à partida, uma vantagem estratégica em bloquear ou interferir na gestão e funcionamento das entidades, organizações ou empresas que suportam as suas próprias infraestruturas.

[243] Cf Alexander KLINBURG, '*Mobilising Cyber Power*', Survival 53, no. 1 (February-March 2011): 41-60; Friedrich WILHELM KRIESEL and David KRIESEL, 'Cyberwar – relevant für Sicherheit und Gesellschaft? Eine Problemanalyse' ('Ciberguerra - relevante para a segurança e sociedade? A análise do problema'), *Zeitschrift für Außenund Sichereitspolitik* 5, no. 4 (2011): 205-16 (214).

O Manual de Tallinn como um primeiro instrumento de trabalho

Esta "ferramenta" constitui um marco na assessoria de agentes políticos, organizações internacionais civis e militares e seus assessores. Foi um trabalho meritório, embora não completo – devido à complexidade dos assuntos, definição dos termos, expressões, procedimentos e também à volatilidade do domínio a que se referem, como já havíamos referido. Também "pecou" pela não participação de outros países da comunidade internacional «da zona diametralmente contrária do espetro (ver p. 35), entre eles, a FR, a China e os membros da OCX, a RFB [e a Índia],» (embora estes possam ser considerados, uma terceira via. Alguns, preconizam um maior multilateralismo na *IG*, mas, internamente, são mais favoráveis a uma «soberania doméstica baseada nos princípios da 'Paz de Vestefália'» (1648) (LOSEY, 2014, pp. 85-86), o que não deixa de ser um contrassenso ou paradoxo). Dos que o encorajaram, nela participaram e o produziram, acharam que valeu o esforço pois, como justifica a informação publicamente veiculada, já se encontra em elaboração uma Versão 2.0 do mesmo, estando prevista a sua publicação durante o primeiro semestre de 2016 pela mesma editora –Cambridge University Press. Este manual –da 1ª Edição– está dividido em duas partes: A primeira abordado legislação de Cibersegurança Internacional, e a segunda relacionada com legislação do Conflito Armado. É composto por sete capítulos e noventa e cinco Regras "de conduta", além de um Glossário de Termos que contribui para a melhoria de rigor nos conceitos e nas definições.

O complemento necessário nos Fóruns Internacionais

O grande desafio que se coloca é uma procura de consensos aceitáveis, pelo menos, que permitam a discussão dos temas, das definições e dos procedimentos mínimos, para que não se comentam "erros grosseiros" de avaliação. A ausência de um conjunto mínimo de entendimento na área do Ciberespaço poderá conduzir a más interpretações de situações que poderão levar a reações tais, que não seja possível um "ponto de retorno". Qualquer uma das potências do Ciberespaço (entre sete e onze países: EUA, República Popular da China (RPC/*People Republic of China–PRC*), FR, Israel, *UK*, Alemanha, França, Índia e, supostamente, RFB, Japão, República da Coreia), com as suas campanhas de *CNE* e algumas de *CNA*, poderão despoletar reações adversas que, no extremo, poderão conduzir a retaliações cinéticas, o que se deverá

evitar a todo o custo, sob pena de desencadear mais um conflito imprevisível na situação atual[244].

Segundo, alguns autores, nota-se na Comunidade Internacional movimentações suficientes de um conflito permanente de "baixa-intensidade" no Ciberdomínio. Por outro, regista-se a existência de uma luta mundial pelo controlo das instituições de *IG* (ver o livro, da Prof, DeNARDIS, Laura, *'The World War for the Internet Governance'*, 2014). Os próximos anos serão decisivos para se confirmar uma escalada de Ciber-armamentos ou se pelo contrário a Comunidade Internacional chega a um consenso mínimo entre o "que é o quê" e o que se poderá utilizar, sem se colocar em risco o desenvolvimento económico e a privacidade. Dever-se-á tentar, também, a diminuição da Ciberespionagem e o Cibercrime, e permitindo, por outro, a utilização de recolha de informações pelo "princípio da reciprocidade". Por fim, nos fóruns internacionais, dever-se-ia pugnar, pela necessária transparência e governação multilateral democrática dos recursos e instituições que participam na Governação da Internet ou *IG*. (ver p. 35)

2.4 Medidas Dissuasoras de Contenção no Ciberespaço

> "No prominent examples have discovered of the European Union (EU) or the North Atlantic Treaty Organization (NATO) conducting its own offensive cyber attacks. On the contrary, their leaders have so far foresworn them." (GEERS, 2013, p. 19) Citando Leyden, J. (6 Jun 2012) "Relax hackers! NATO has no cyber-attack plans-top brass." *The Register*

> "Cyber war [conflict] can be managed through inter-state deterrence, and offensive capabilities plus resilience, if deterrence fails." (NYE Jr., "Cyber Power", 2010, p. 16), citando Richard A. CLARK and Robert K. KNABE, *Cyber War: The Next Threat to National Security and What to Do About It*, (New York: Harper Collins, 2010)

> "*Building deterrence is necessary, including offensive cyber capabilities*. Every state or alliance of states needs some level of deterrence to be credible. The discussion must also address the question of who will build these capabilities – every state, an alliance of states or the private sector? Should it be legal for the private sector firms to sell one-use offensive cyber weapons to the highest bidder? In the sphere of military cyber defence cooperation, the only logical partner for Eurpean states, including Finland

[244] "This means that China's alleged incursions are not the only threat; America's increasingly forceful position on cyber espionage could inadvertently trigger a cyber war. After all, actions about cyberspace can be misunderstood just as easily as activities in cyberspace." Read more at http://www.project-syndicate.org/commentary/the-threat-of-an-accidental-cyber-war-by-alexander-klimburg-and-franz-stefan-gady#rxzyBdcJ8PFHs1sT.99

> [um País «neutral»], is NATO [porque, é parceiro e pretence à UE].” (SALONIOUS-PASTERNAK & LIMMÉIL, 2012, p. 7)

Existem três fatores estratégicos a ter em consideração na definição de uma verdadeira política de Cibersegurança para a Europa, em geral, e para a UE, em particular: O primeiro, apesar de ser verdade uma crescente translação da preponderância económica e financeira do Atlântico para o Pacífico –devido à força da Globalização e da deslocalização de empresas desta área para a Ásia/Pacífico–, o remanescente “peso” das economias da zona Euro-Atlântica continuará a ser muito significativo, devido à sua especialização ligada à tecnologia, informação, conhecimento, e às interligações, cada vez maiores, desta com a economia real; O segundo, a *gap* [245] existente na implementação de estratégias de Cibersegurança entre os EUA e a Europa –das que existem, em cada um dos países ou EMs da UE ou dela mesma, e são do domínio público– é significativa. Se não houver vontade política e o respetivo investimento –difícil de concretizar, devido à racionalização de recursos e subalternização da defesa e da segurança em época de crise grave, assim como, uma melhoria no nível de coordenação–, ela acentuar-se-á. Como consequência disso, os EUA ficarão, é certo, com menos espaço de manobra nos fóruns internacionais, mas mais imunes a Ciberataques. A Europa, pelo contrário, será considerada mais vulnerável. Logo, a probabilidade de ser vítima de novos e mais sofisticados ataques aumentará necessariamente; Em terceiro e último, a proliferação de ciberestratégias operacionais na Europa e na UE –o Reino Unido na dianteira procurando seguir a dos EUA–, a Alemanha[246] e a França de “costas-voltadas”[247] –na continuação do que ocorreu, recentemente, na intervenção na Líbia–, e os restantes países, “cada um por si”, ou dependentes de terceiros, como reflexo da descoordenação e da ineficiência da PESC. Apesar do profissionalismo, esforço e boa vontade da *ENISA*, por si só, não será suficiente a Resiliência para tornar a UE um alvo menos vulnerável a nível global, muito pelo contrário. Para completar, será muito difícil e impensável à partida, no

[245] “The difference between the United States and Europe is notable, and without serious efforts in Europe, the gap is only likely to widen. This would increase the potential for Europe to become the focal point for serious cybercrime, espionage and even debilitating attacks.” (SALONIOUS-PASTERNAK & LIMMÉIL, 2012, p. 2) .”

[246] http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html e http://www.spiegel.de/international/world/germany-increases-counterintelligence-in-response-to-us-spying-a-982135.html , Consultados a 15/ago./2014.

[247] “By 2007 the Alliance was strained by Jacques Chirac’s Gaullism and strict guidelines for Bundeswehr operations […]” (LAASME, 2012, p. 14)

quadro atual –por exemplo– um consenso na UE sobre o desenvolvimento de capacidades ofensivas para a área do Ciberespaço, como forma de impor o conceito de *deterrence*, tão necessário, em cenários prováveis de incremento de risco próximo-futuro (quando ações anteriores, menos "melindrosas", não tiveram sucesso e geraram mesmo retaliações a EMs da União, por exemplo, Estónia, Holanda, Dinamarca, etc.). Isto, porque «a dissuasão[248] é uma mistura de considerações políticas e militares» [citando GEERS, Keneth[249] (CALDAS & FREIRE, 2013, p. 12)], diríamos mesmo que ao nível da UE, predominantemente políticas. Sendo assim, parece-nos extremamente complicado, chegar-se a um consenso ao nível do Conselho, devido aos interesses particulares dos EMs –no plano das suas políticas externas–, já para não falarmos no PE –com a configuração, atual, saída das últimas eleições de maio, em que uma possível maioria de suporte será menos qualificada, devido à polarização, quer à esquerda, mas, particularmente, à direita com o incremento de deputados e grupos, designados de forma genérica, de "eurocéticos"–, de haver a "coragem" política para adotar medidas de dissuasão ou *deterrence* que se sobreponham aos interesses dos EMs.

Elementos dissuasores como complemento de Resiliência

A posição da UE no quadro internacional como ator estratégico está condicionada a vários elementos de vulnerabilidade. Em particular no plano da Ação Externa e do instrumento com essa função –o SEAE– será necessária a sua funcionalidade plena e permanente, quer em tempo de paz e cooperação, como em tempo de intervenções inerentes à implementação de ações no quadro da PESC –de

[248] "A dissuasão proposta por Keneth Geers prevê duas metodologias: a negação de aquisição de tecnologias ameaçantes e a punição. O autor procede a essa análise sob as perspetivas de capacidade, credibilidade e da comunicação/visibilidade. Considerando dois aspetos desafiantes ao nível de ciberataques, que são a atribuição dos ataques e a sua assimetria, infere que a dissuasão é uma tarefa praticamente impossível. Por exemplo, o principal desafio da anti proliferação é definir o código comprometido|[de comprometimento], porque podem ser usados caminhos legítimos para roubar segredos nacionais. Mesmo para os especialistas poderá ser tarefa 'exigente' identificar o 'erro' no meio da análise de um elevado número de linhas de código. Assim, proibir o desenvolvimento de ciberataques via Tratados Internacionais pode até banir iniciativas de ataque e de disrupção de redes não combatentes mas aumenta a gestão internacional da internet (se é que existe) e pouco melhora no problema essencial, a questão das atribuições. No que respeita à dissuasão com recurso à punição esta tem de ser entendida como último recurso, e só depois de esgotados os instrumentos da negação. A punição tem como objetivo a prevenção da agressão com a ameaça de uma maior agressão, tida como dolorosa ou de retaliação. Isso significa que o agressor tem de ficar convencido que a vitória não é possível. Normalmente, os aspetos da atribuição e da assimetria estão em causa. Na parte relativa à atribuição, a capacidade de responder está posta em causa* por dificuldade da sua identificação. No respeitante à assimetria está comprometida a credibilidade com a desproporção dos meios." (CALDAS & FREIRE, 2013, p. 13)

[249] Num trabalho intitulado '*Strategic Cyber Security'*, 2011, disponível em www.ccdcoe.org/278.html, CCDCoE, onde as abordagens são bem refletidas pese embora tenha como enquadramento os EUA. Consultado a 27/jan./2014.

segurança humanitária, de retorno a situações de normalidade democrática, etc.– ou ainda, em extremo, no apoio a ações de vetor mais "militarizado" no quadro da PDSC, como instrumento externo da PESC. Este conjunto abrangente de funções exige cada vez mais uma presença sólida e permanente no quinto domínio de operações –o Ciberespaço. A UE necessita com urgência e com solidez de desenvolver procedimentos e ferramentas que permitam operar com toda a segurança e autonomia no Ciberespaço em geral e na Internet, em particular, fora do espaço físico da UE. Só assim, poderá o SEAE levar a cabo as ações que lhe são confiadas sem ser necessário a intervenção de outras organizações internacionais de quaisquer naturezas. Isto só poderá acontecer com uma estratégia inequívoca que aposte em tecnologias concebidas e produzidas na UE, nomeadamente, com o suporte da AED. No entanto, existe todo um trabalho e experiência adquirida pela NATO, particularmente, em Dissuasão. Estas ferramentas baseadas na filosofia de *CNO* –enquadradas como uma componente no conceito lato de Cibersegurança– permitiriam, por exemplo, aproveitar a pertença de grande maioria dos EMs da UE, serem-no, também, da OTAN, como já se havia dito, procurando sinergias comuns, racionalizando custos e justificando para a Opinião Pública as verbas –alocadas a estes projetos–dos orçamentos pagos pelos contribuintes dos membros UE–OTAN.

Recomendações e Conclusões

> "The Union's cyber security policy may still be in its infancy and hampered by difficulties, but the EU could yet become a key player in the field – if it plays its cards wisely. While the US has been seriously hit by the scandal surrounding the secret NSA surveillance programmes, the struggle over how to frame internet governance goes on and, more than ever, needs core stakeholders capable of defending freedom, democracy and the rule of law in cyberspace. The EU's longstanding commitment to those values in its foreign policy and unquestioned leadership in data protection mean it is well placed to play a significant role therein." (PAWLAK, 2013, p. 1)

Num trabalho desta natureza –de análise aprofundada quando possível (dependendo das fontes secundárias disponíveis, na impossibilidade orçamental e operacional de consultar fontes primárias, distantes e algumas confidenciais) e transversal, devido à natureza do domínio relacionado com o subcampo em análise (intercetar as dimensões civis e militares, políticas e económicas, nacionais e internacionais)– é deveras audaz, mas necessário, avançar recomendações e, com maioria de razão, algumas afirmações conclusivas a respeito, embora condicionadas.

Devemos ter em consideração que, em geral, o subcampo em análise –da segurança no domínio do Ciberespaço– ser, relativamente, recente (de vinte a trinta anos). No que ao trabalho diz respeito –à Europa, UE e NATO–, o hiato de tempo reduz-se para –dez a quinze anos– sendo um período relativamente curto. Estas razões trazem várias implicações ao nível do rigor dos conceitos e da solidez das definições associadas às problemáticas do subcampo, conduzindo a possíveis "erros de paralaxe" nos processos de análise relativos aos atores envolvidos, aos fenómenos existentes, aos processos de funcionamento, às consequências dos procedimentos e suas implicações na dimensão política das organizações UE e OTAN.

Mesmo assim, existe de forma legível, três recomendações de Avaliação de Ativos da UE que podem ser –sem corrermos o risco de exagerar– registadas em relação ao trinómio UE-OTAN-*IG* e que deverão ser exploradas em toda a sua extensão.

Recomendações na Avaliação de Ativos da União Europeia

> "The nascent institutional structure of global Internet regulation is very important in view of the EU´s own regulation efforts. The Union and its member states take part in almost all of the above-mentioned institutions [*IETF, IEEE, ICANN, ICSPA, FS-ISAC, IG-UTI, etc.*] and use these as platforms to cooperate with one another as well as with other states. However, the Union is not only another actor within the global institutional landscape, but also constitutes a highly developed institutional framework for formulating cross-border policies, the EU is something of a model for what takes place on a global scale: developments that we witness in the EU today can be seen as a precursor of developments at the international level. The internal dynamics of the EU can thus give interesting insight into the future perspectives of global Internet regulation. In fact, the dynamics of global cyber security policy are often identical to those in the EU" (BENDIEK, "European Cyber Security Policy", 2012, p. 19)

1. A UE como laboratório de possíveis soluções globais de *IG* no Ciberespaço

A UE como maior "Comunidade Regional" em funcionamento, poderá e deverá constituir um espaço priveligiado de conceção e implementação de políticas para o Ciberespaço. Devido à natureza particular da sua arquitetura de Governação, da pluralidade de culturas e experiências democráticas, da extensão geográfica, do número de consumidores e de utilizadores de Internet e do seu não linear percurso de construção comunitário, da sua participação em fóruns internacionais, da sua postura multilateral democrática, a UE é um «laboratório» em potência para a procura de soluções –hoje– para possível aplicação a outras "comunidades" regionais e, quem sabe, extensíveis ao Globo. Este consitui o maior ativo que a UE detém, e que deverá ser plenamente explorado, quer nos planos nacionais dos EMs, na União e a nível internacional.

2. A incontornável parceria UE-OTAN, também, no Ciberespaço

A OTAN como instituição sexagenária de fornecimento de serviços de Defesa e Segurança –em particular no espaço Euro-atlântico Norte– constitui uma base sólida para o estabelecimento de parcerias com outras instituições internacionais, nomedamente, a UE. Atendendo a que a grande maioria dos EMs da UE são-no de igual forma da OTAN, ou, pelo menos, quando têm o estatuto de parceiro da organização. Por essa razão, seria despiciente para ambas as organizações não aproveitar a pertença recíproca de grande parte dos seus membros. Esse alheamento seria inexplicável para a

Opinião Pública por si só, sendo na conjuntura atual de restrições orçamentais, completamente inconsebível. Assim, o aproveitamento de sinergias e de experiências da OTAN –sempre que isso seja possível, deveríam ser aproveitas pela UE, principalmente ao nível da Resiliência e da utilização de medidas de dissuasão– em ações do SEAE, em operações da PESC e, mesmo, da PCSD. Isto, como é óbvio, sem comprometer o conjuto de mais-valias resultantes do ativo principal atrás descrito, muito pelo contrário, incentivando outros a seguirem o multilateralismo democrático.

3. A necessidade imperiosa de Multiralismo na *IG* e o papel fulcral da UE

Como consequência da primeira recomendação –e por maioria de razão– a UE deverá constitui-se como o principal catalizador na conceção e implementação de políticas para o Ciberespaço ao nível Global, em particular na *IG*, procurando projetar os seus Valores Fundamentais na procura de um equilíbrio entre a Segurança do Ciberespaço e um padrão de mínimos de Privacidade dos cidadãos e saudável convivência da Comunidade Internacional. De prefência, deverá procurar incentivar o Multilateralismo em todos os fóruns internacionais em que participe, como primeira prioridade, dos seus objetivos estratégicos para o Ciberespaço e Internet, defendendo os Direitos Humanos, a Privacidade e a Proteção de Dados, a transparência e a democracia.

Conclusões

> "[…] But many examples reveal European networks getting hacked from other parts of the world, particularly China and Russia. […] in 2011, European Commission officials were targeted at an Internet Governance Forum (IGF) in Azerbaijan. […] In business, the European Union's carbon trading market was breached in 2011, resulting in the theft of more than $7 million in credits, forcing the market to shut down temporarily. […]" (GEERS, 2013, p. 19)

> "In case of an armed conflict, information warfare is destined to play a key role, as almost all military capabilities now rely in one way or another on information technology. As a result, conflicts between major powers are unlikely to be limited to operations on conventional battlefield. Sandro Gaycken underlines the significance of information technology for modern warfare by pointing out that 'in a way, cyber warfare enables the return of war despite the impossibility of major conventional conflicts.[250]" (BENDIEK, "European Cyber Security Policy", 2012, p. 11)

> "The lack of international consensus on definitions of cyber offences is not the result of disputes over technical and legal subtleties, but reflects a fundamental disagreement regarding the appropriateness and proper scope of government regulation in this policy field.[*] While some support the idea of establishing a centralised intergovernmental organization for Internet oversight, others favour a descentralised, multi-stakeholder governance model based on equal partnership between government, private sector, civil society, and technical experts.[**251]" (BENDIEK, "European Cyber Security Policy", 2012, pp. 7-8)

Este trabalho procurou, em primeiro lugar, fazer uma resenha histórica do aparecimento da problemática da segurança do Ciberespaço na UE como reflexo de condicionalismos externos –implosão da URSS, incremento do crime organizado de

---

[250] "[*]Interview with Sandro Gayken, 'Mit Cyber-Kriegen lassen sich geostrategische Ziele realisieren' (A ciberguerra pode ser utilizada para a realização de objetivos geoestraégicos), Zeit Online, 8 February 2012 (quote translated by T.I.M.)."

[251] "[*]According to KLEINWÄCHTER, 'three layers play a role in Internet regulation: the transport layer, i.e. the telecommunications infrastructure, that is regulated by national telecommunications law as well as by international treaties negotiated in the framework of the ITU [International Communication Union]; the protocol layer – in the stricter sense, «the Internet» with its codes, standards, IP addresses and domain name systems – that is regulated by non-governmental global institutions such as the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), the Institute of Electrical and Electronics Engineers (IEEE), the Internet Corporation for Assigned Names and Numbers (ICANM) or the Regional Internet Registers (RIRs); application Layer – i.e. all web-based services from e-commerce to social networks, which are primarily regulated by national law and, furthermore, by constitutional law, including freddom of expression and protection of property and privacy' Wolfgang KLEINWÄCHTER, 'Wie reguliert man den Cyberspace? Die Quadratur des Dreiecks" (Como regular o Ciberespaço? Quadratura do triângulo.), *Heise On-line- Telepolis*, 29 May 2012, thhp://www.heise.de/tp/druck/mb/artikel/34/34742/1.html (acessed on 2 June 2012; quote translated by T.I.M.).[**] Cf. Wolfgang KLEINWÄCHTER, "Kalter Krieg im Cyberspace oder konstruktiver Dialog? Auslick auf die Internetpolitik 2012" (Guerra Fria no Ciberespaço ou diálogo construtivo? Ver a Política de internet 2012), *Heise On-line- Telepolis*, 29 May 2012, thhp://www.heise.de/tp/druck/mb/artikel/36/36266/1.html (acessed on 17 March 2012))"[252] KLIMBURG, Alexander, Watson Institute/Universidade de Brown em 20/mar/2013 Ver diapositivo n.º 6 aos 05':16" até 06':16" em https://mediacapture.brown.edu:8443/ess/echo/presentation/8792278f-7098-40ec-87a7-a51ac98c49fa Consultado a 23/set/2014.

índole eletrónica, recomendações da *INTERPOL* e preocupações do CdE colocadas em Convenção sobre o Cibercrime– e preocupações internas –relacionadas com a luta contra a infoexclusão, a economia do conhecimento e crescimento económico, em suma, a sociedade de informação–, durante aquilo que se poderá designar pela **Fase – I**.

Foi sintomático que a UE entrou, verdadeiramente, numa **FASE – II** em 2007. Notou-se uma separação clara entre as preocupações da fase anterior e o incremento de vulnerabilidades –em complexidade e escala de perigosidade– após os acontecimentos ocorridos –no Ciberespaço– na Estónia e confirmados no ano seguinte, na Georgia. Tomou a UE consciência que seria útil e necessário separar as preocupações com a *eSociety* da proteção das Infraestruturas vitais das sociedades democráticas modernas. Esta preocupação já tinha sido sentida na margem americana do Atlântico, pelo menos, uma década antes, tendo-se agravado com os acontecimentos nefastos do *09/11*. Daí à criação de uma *Framework* de proteção de Sistemas e Redes de Informação foi um passo. Ela já se encontrava em gestação com a criação da *ENISA* em 2004. Após 2007, a *ENISA* tem vindo a ter um papel predominante na definição e implementação do conceito de Resiliência na União, plenamente confirmado com a extensão do seu mandato e áreas de intervenção até 2020. Porque tão importante como as PICs, a UE criou o *E3C* dependente da *EUROPOL*, sedeado em Haia, para melhorar as RSIs, relativamente ao combate ao "mega" Cibercrime.

Com a entrada em funções da CE–"Barroso II", começaram as preparações para a entrada em funcionamento do quadro de referência e de ferramentas que na área do Ciberespaço. Falamos de dois instrumentos fundamentais: A Agenda Digital e a ECS da UE. No entanto, e devido à complexidade das matérias em causa, da pluralidade democrática, da arquitetura de governação da UE, de pressões externas –estatais e corporativas– isso não foi possível. **Eis chegados a uma primeira conclusão: o percurso de implementação das políticas de Cibersegurança na UE tem sido enviesado, complexo e difícil**. Isto tem sido devido a razões de funcionamento interno –descoordenação, sobreposição de instituições e de políticas por vezes contraproducentes–, e a condicionalismos de pressão externos –muitas vezes inexplicáveis e pouco transparentes– numa comunidade composta por EMs democráticos, mas com interesses díspares, agendas muito próprias, que inibem os objetivos por eles mesmos definidos em Conselho, e com amplas maiorias no PE. Mas a

construção de uma verdadeira Segurança para o Ciberespaço na UE passa, segundo alguns autores[252], por três níveis: «Coordenação dos/nos Governos» dos EMs, onde conta o "elo mais fraco" do sistema; «Colaboração Internacional», com uma participação atenta e ativa nos vários fóruns –desde o mais importante, a ONU, passando por aqueles de significância reduzida– porque os problemas de hoje sê-lo-ão muito maiores amanhã, se não se procurarem, desde logo, soluções de compromisso; e, não menos importante, «Cooperação na própria UE» e dos seus relacionamentos internos institucionais: com os EMs, ao nível do Conselho, no PE e suas relações com os Parlamentos Nacionais e, muito em especial, com a Sociedade Civil europeia, as ONGs –nacionais, do espaço da União e extracomunitário– não esquecendo o setor privado da economia. **Assim chegamos a uma segunda conclusão: a UE só estará apta a ser considerada um parceiro Global na área da Cibersegurança se começar a trabalhar internamente numa Fase – III**, que atingirá, estamos certos, quando for capaz de:

- Resolver os problemas pendentes e relacionados com a Agenda Digital e colocando o Mercado Único Digital plenamente funcional;
- Conseguir estabelecer um padrão mínimo de Cibersegurança em todos os EMs, –incluindo, as instituições da União– e proceder à sua monitorização e correção de forma sistemática e inteligente, consolidando o seu *Cyberpower*;
  Aplicar este *Cyberpower* a um SEAE plenamente operativo e funcional, capaz de implementar a UE-ECS ao nível da PESC e da PCSD. Para esse efeito, a AED poderá recorrer a parcerias com a OTAN, na aquisição de sinergias relativas a mecanismos de dissuasão, caso falhe a, necessária, e fundamental, Resiliência –conseguida pelo pontos anteriores, pela *ENISA*, *E3C*, etc.– e a, complementar, uma Diplomacia consolidada pelo *Softpower* da UE.

[252] KLIMBURG, Alexander, Watson Institute/Universidade de Brown em 20/mar/2013 Ver diapositivo n.º 6 aos 05':16" até 06':16" em https://mediacapture.brown.edu:8443/ess/echo/presentation/8792278f-7098-40ec-87a7-a51ac98c49fa Consultado a 23/set/2014.

Bibliografia

BRZEZINSKI, Z. (2012). *Strategic Vision – America and the Crisis of Global Power.* New York: Basic Books.

COHEN-TANUGI, L. (2007). *Guerre ou paix - Essai sur le monde de demain* (éd. 1 er, Vol. 25 em). (J. Roman, Éd.) Paris: Hachette Littératures.

ETZONI, A. (2011). Nationalism: The Communitarian Block. *Brown Journal of World Affairs , XVIII, ISSUE I* (Sociologia), 229-247.

HEALEY, J. (2011, out). "The Spectrum of National Responsability for Cyberattacks". *Brown Journal of World Affairs , XVIII*, pp. 57-70.

HERRERA, G. L. (2007). Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space. In P. a. age, & M. D. Cavelty (Ed.), *Power and security in the information age", Chapter 4 Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space Geoffrey L. Herrera (Hampshire: Ashgate Publishing, 2007) p. 67.* Hampshire: Ashgate Publishing.

LIBICKI, M. C. (FALL/WINTER 2011). "The Nature of Strategic Instability in Cyberspace". *Brown Journal of Foreign Affairs .*

NYE Jr., J. S. (2012). *O Futuro do Poder* (1.ª março de 2012 ed.). (L. O. Santos, Trad.) Lisboa: Temas e Debates.

ROSENZWEIG, P. (2013). *Thinking about Cybersecurity: From Cyber Crime to Cyber Warfare* (The Grate Courses ed.). Chantilly, Virginia 20151-2299 (VA), USA: The Teaching Company - Corp. HQ, 4840 Westfields Boulevard, Suite 500.

SCHMIDT, H. (2011, abr 11). "Defending Cyberspace: The view from Washington". *Brown Journal of World Affairs , XVIII*, pp. 49-55.

Webgrafia

AALTOLA, M., SIPILÄ, J., & VUORISALO, V. (2011, jun 09). Retrieved jan 19, 2013, from THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS: www.fiia.fi

Agence Nationale de la Sécurité des Systèmes d'Information. (2011, fev). Consulté le jan 17, 2013, sur www.ssi.gouv.fr.

BEJARANO, M. J. (28 de mar de 2012). *Ciberdefensa, Equipos de Respuesta Inmediata de la OTAN*. Obtido em 22 de mai de 2013, de Istituto Español de Estudos Estratégicos: www.ieee.es/Galeris/fichero/docs_informativos/2012/DIEFEI16-2012_NatoRapidReactionTeam_MJCaro.pdf

BENDIEK, A. (out de 2012). *Stiftung Wissenschaft und PolitikSWP Research Paper*. Obtido em 24 de jan de 2014, de German Institute for International and Security Affairs: www.swp-berlin.org

BENDIEK, A., & PORTER, A. L. (2013). European Cyber Security within a Global Multistakeholder Structure. *European Foreign Affairs Reviw , 18*, pp. 155 - 180.

BISCOP, S. (2012, nov). *Security Policy Brief*. Retrieved fev 18, 2014, from Egmont Royal Institute for International Relations: www.egmontinstitute.be

BRUNNER, E. M., & GIROUX, J. (2009, set). *CSS Analysis in Security Policy*. Retrieved mai 03, 2013, from Center for Security Studies (CSS), ETH Zurich: www.ssn.ethz.ch

CALDAS, A., & FREIRE, V. (2013). *E-Briefing Papers - http://www.idn.gov.pt/index.php?mod=1410&area=1100*. (A. CARRIÇO, Ed.) Obtido em 17 de jun de 2014, de Instituto de Defesa Nacional - IDN - www.idn.gov.pt: http://www.idn.gov.pt/conteudos/documentos/e-briefing_papers/Working_Paper_2_Ciberseguranca.pdf

CAVELTY, M. D. (2012, mar). "The militarisation of cyber security as a source of global tension". (D. Möckli, Ed.) *Strategic Trends 2012* , pp. 103-124.

CAVELTY, M. D. (2013, dec). Retrieved fev 17, 2014, from Swedish Institute of Foreign Affairs: www.ui.se

CAVELTY, M. D. (2011, mar). Cyber-Allies : Strengths and weaknesses of NATO's cyberdefense posture. *IP - Global Edition* , pp. 11 - 15.

CAVELTY, M. D. (2010, abr). *www.sta.ethz.ch.* Retrieved jan 11, 2013, from www.ssn.ethz.ch.

CAVELTY, M. D., & PRIOR, T. (2012?, out). *CSS Analysis in Security Policy.* Retrieved mai 03, 2013, from Center for Security Studies (CSS), ETH Zurich: www.css.ethz.ch/cssanalysen

CAVELTY, M. D., & SUTER, M. (2009, ago 27). *academia.edu.* Retrieved fev 22, 2014, from ELSIVER: www.elsiver.com/locate/ijcip

Council of the European Union. (2013, jun). *General Affairs Council meeting, Luxembourg, 25 June 2013.* Retrieved out 05, 2013, from Council of the European Union: www.consilium.europa.eu/endocs/cms_data/docs/pressdata/en/jha/137602.pdf

ERIKSSON, J., & NOREEN, E. (2002). *Dept. of Peace and Conflict Research, Uppsala University.* Retrieved jun 08, 2013, from Uppsala University: http://www.uu.se/digitalAssets/18/18591_uprp_no_6.pdf

European Network and Information Security Agency ENISA. (2012, mai 08). *Resillience and CIIP Program at ENISA.* Retrieved abr 02, 2014, from ENISA: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport

Federal Ministry of the Interior. (2011, fev). Retrieved jan 18, 2013, from www.bmi.bund.de.

GEERS, K. (2013, set 30). *Blog - Threat Intelligence.* Retrieved out 11, 2013, from Fire Eye: http://www.fireeye.com/blog/technical/threat-intelligence/2013/09/new-fireeye-report-world-war-c.html

HAWKES, B. (21 de July de 2014). *Institute of International and European Affairs - IIEA.* (I. D. Commissioner, Ed.) Obtido em 28 de julho de 2014, de Institute of International and European Affairs - IIEA: http://www.iiea.com/events/keynote-address-billy-hawkes

HELMBRECHT, U. (2013, fev 19). ENISA's mandate has just been renewed, giving it the green light to continue its work for the next seven years. (J. Baker, Interviewer) vieuws - The EU Policy Broadcaster.

HIGH REPRESENTATIVE/VICE PRESIDENT. (2013, fev 07). *Access to European Union law - Document Join (2023) 1 FINAL.* (H. R. Commission, Ed.) Retrieved out 11, 2013, from Euro-Lex Access to European Union law: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=JOIN:2013:0001:FIN:EN:PDF

HORGBY, A., & RHINARD, M. (2013, dec). *UI Occasional papres.* Retrieved mar 17, 2014, from The Swedish Institute of International Affairs: www.UI.se

HYPÖNNEN, M. (2013, out). *How the NSA betrayed the world's trust — time to act.* Retrieved nov 11, 2013, from TED Ideas Worth Spreading: http://www.ted.com/talks/mikko_hypponen_how_the_nsa_betrayed_the_world_s_trust_time_to_act

Instituto de Defesa Nacional. (dec de 2013). (A. CARRIÇO, Ed.) Obtido em 12 de mar de 2014, de Instituto de Defesa Nacional: www.idn.gov.pt

KEOHANE, R. O., & NYE JR., J. S. (1998, set/out). Retrieved mar 27, 2013, from www.foreignaffairs.com.

KLIMBURG, A., & TIIRMMA-KLAAR, H. (2011). *DG Ext. Policies - Policy Dep.* Retrieved jan 08, 2014, from European Parliament - Directorate-General for External Policies - Policy Department: http://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/433828/EXPO-SEDE_ET%282011%29433828_EN.pdf

KNABE, R. K. (5 de July de 2010). Obtido em 16 de setembro de 2014, de Council on Foreign Relations: http://www.cfr.org/united-states/untangling-attribution-moving-accountabilitycyberspace/

LAASME, H. (2012, dez). *Great Debate Paper.* Retrieved nov 18, 2013, from Cicero Foundation - An Independent Pro-EU & Pro-Atlantic Think-Tank: www.cicerofoundation.org/lectures/Laasme_%20Estonia_NATO_Cyber_%20Strategy.pdf

LOSEY, J. (ago de 2014). *James Losey*. Obtido em 28 de ago de 2014, de academia.edu: http://www.academia.edu/813357/Towards_Information_Interdependece

MASCOLO, G., & SCOTT, B. (October de 2013). *New American Foundation+Open Technology Institute + Wilson Center*. Obtido em 09 de setembro de 2014, de Wilson Center: www.wilsoncenter.org/sites/default/files/NAF-OTI-WC-SummerofSnowdenPaper.pdf

Military-Balance Online, T. &. (Ed.). (2013, 03 14). *The Military Balance 2013*. Retrieved 05 28, 2013, from http://www.tandfonline.com/page/terms-and-conditions: http://dx.doi.org/10.1080/04597222.2013.756999

MORAES, Claude. (21 de fev de 2014). Obtido em 27 de fev de 2014

MUELLER, B. (June de 2014). Obtido em 16 de setembro de 2014, de The London School of Economics and Political Science: http://www.lse.ac.uk/IDEAS/publications/reports/SU14_2.aspx

NATO A- Z. (n.d.). *NATO and cyber defence*. Retrieved jun 22, 2013, from NATO live: http://www.nato.int/cps/en/natolive/topics_78170.htm

NOTO, N. D. (2013, set). *http://www.fscpo.unict.it/*. (r. a. The ReSHAPE Research Project on "EU and the multilateral policies for disater prevention, Ed.) Retrieved fev 14, 2014, from Dipartamento di Scienze Politiche e Sociali: www.fscpo.unict.it/EUROPA/JMAP/repaper5.pdf

NUNES, I. F. (2012). *Policy Papers do IDN*. Obtido em 04 de mai de 2014, de IDN - Instituto de Defesa Nacional: http://www.idn.gov.pt

NYE Jr., J. S. (2010). "Cyber Power". *Harvard Kennedy School - Belfer Center for Science and International Affairs* .

PAWLAK, P. (2013, set 18). *Brief Publications*. (EUISS, Ed.) Retrieved jan 30, 2014, from European Union Institute for Security Studies: http://www.iss.europa.eu/publications/detail/article/cyber-world-site-under-construction/

RAND Europe. (2012, fev). *http://www.rand.org/pubs/technical_reports/TR1218.html.* Retrieved fev 18, 2014, from www.rand.org: http://www.rand.org/content/dam/rand/pubs/technical_reports/2012/RAND_TR1218.pdf

RASMUSSEN, A. F. (2013). *"The Secretary General's Annual Repport 2012"*. Retrieved mai 8, 2013, from NATO Revew Magazine: http://www.nato.int/docu/review/2012/Predictions-2013/SGReport/EN/index.htm

RATTRAY, G. J., & HEALEY, J. (June de 2011). http://mercury.ethz.ch/serviceengine/Files/ISN/129918/ichaptersection_singledocument/d157a5f2-4963-4770-8de0-a7c2bab6db2a/en/Chapt5.pdf Obtido em 08 de dezembro de 2013

SALONIOUS-PASTERNAK, C., & LIMMÉIL, J. (2012, dez 12). *Transatlantic cybersecurity:The only winning move is to play with others.* Retrieved mai 22, 2013, from The Finnish Institute of international Affairs: http://www.fiia.fi/en/publication/303/transatlantic_cybersecurity/

SCHAAKE, M. (15 de November de 2013). *Irish Institute of European Affairs - IIEA Cybersecurity Conference* . Obtido em 05 de agosto de 2014, de Irish Institute of European Affairs: https://www.youtube.com/watch?v=u6rd3qvXJFQ

SCHMITT, M. N., & VIHUL, L. (Spring de 2014). *Fletcher Security Review.* Obtido em 09 de setembro de 2014, de Columbia International Affairs online.

TABANSKY, L. (2014, mai). *Cyber Security Review.* (T. PARTRIDGE, Ed.) Retrieved jun 03, 2014, from www.deltabusinessmedia.com: www.cybersecurity-review.com

THE WHITE HOUSE. (2011). *USA International Strategy for Cyberspace.* Washington: The White House.

TIIRMAA-KLAAR, H. (15 de Nov de 2013). *Irish Institute of External Affairs - IIEA, Cybersecurity Conference*. Obtido em 10 de junho de 2014, de Irish Institute of External Affairs - IIEA: http://www.youtube.com/watch?v=gyPsx1EyNfL