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)