UNIVERSIDADE DOS AÇORES
FACULDADE DE CIÊNCIAS SOCIAIS E HUMANAS

‘’ A ameaça iminente do *cyberterrorismo* - O bem-estar das relações internacionais’’

Dissertação de Mestrado

Maria Carolina Silva Gomes de Menezes

MESTRADO EM:

Relações Internacionais: O Espaço Euro-Atlântico

Ponta Delgada, 2022

‘’ A ameaça iminente do *cyberterrorismo* - O bem-estar das relações internacionais’’

Dissertação de Mestrado

Maria Carolina Silva Gomes de Menezes

Orientador

Prof. Doutor Luís Manuel Vieira de Andrade

Dissertação apresentada à Universidade dos Açores para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Relações Internacionais: o Espaço Euro-Atlântico

Agradecimentos

À minha avó Helena, que tão generosamente me ofereceu o mestrado numa área que tanto me diz,

À minha mãe e ao meu pai que sempre me apoiaram na elaboração desta dissertação e que sempre acreditaram na minha capacidade de a fazer com rigor e brio,

Ao meu irmão que me ajudou incansavelmente a procurar informação e bibliografia sobre a matéria em questão,

Ao meu namorado que me deu muita força e motivação para que terminasse o mestrado com boa média, e fizesse a dissertação a tempo,

O meu muito obrigada, sem vocês não teria sido possível.

Resumo

A Ameaça Iminente do Ciberterrorismo – O impacto nas Relações Internacionais

Maria Carolina Silva Gomes de Menezes

A 6 de agosto de 1991, há 21 anos atrás, a *World Wide Web* ficou disponível mundialmente, havendo agora quase 4.3 biliões de pessoas a utilizá-la diariamente. Com ela, vieram diferentes vantagens, tais como a capacidade de resolver problemas burocráticos através de um clique, ou a facilidade de procura de informação, bem como a proximidade e globalização que permite acontecer. No entanto, existe sempre ‘’o outro lado da moeda’’.

Ultimamente, o investimento em armamento e forças militares, além da corrida ao poder nuclear têm vindo a decrescer, face ao que outrora foi, uma vez que os governos cada vez mais têm a plena noção de que tais custos implicam grandes endividamentos, e um peso insuportável, não só a nível económico, como também a nível de recursos humanos. No entanto, e com o evoluir da tecnologia e internet, é possível travar guerras e atacar inimigos silenciosamente.

Tenciona-se investigar e aprofundar o fenómeno que é a internet e o impacto que os problemas advindos da mesma causam nos dias de hoje, nomeadamente nas relações internacionais. Serão analisados, por isso, e com maior detalhe e rigor o *ciberterrorismo, o ciberespaço* e, por consequência, a *cibersegurança,* no âmbito da matéria em vista.

O período temporal que será alvo de estudo nesta dissertação vai desde a primeira guerra cibernética em 1999, até às eleições de Donald Trump em 2016, estendendo-se até aos dias de hoje.

Pretende-se compreender o porquê da mudança e opção pelo *ciberterrorismo* nas últimas décadas e o impacto do mesmo nas relações internacionais atualmente. Dado que não se trata só de ataques internacionais, mas até mesmo de pessoas coletivas face ao estado, ou outras entidades coletivas, será oportuno estudar os vários casos possíveis e marcantes em que tais situações aconteceram.

Palavras Chave: Internet; Ciberterrorismo; Ciberespaço e Cibersegurança.

Abstract

The Imminent Threat of Cyberterrorism – The Impact on International Relations

Maria Carolina Silva Gomes de Menezes

On August 6, 1991, 21 years ago, the World Wide Web became available worldwide, with nearly 4.3 billion people now using it daily. With it came different advantages, such as the ability to solve bureaucratic problems with a click, or the ease of searching for information, as well as the proximity and globalization that allows this to happen. However, everything has "the other side of the coin".

Lately, investment in armaments and military forces, in addition to the race for nuclear power, has been decreasing, compared to what it used to be, since governments are increasingly aware that such costs imply large indebtedness, and a weight unbearable, not only economically, but also in terms of human resources. However, and with the evolution of technology and internet, it is possible to wage wars and attack enemies silently.

It is intended to investigate and deepen the phenomenon that is the internet and the impact that the problems arising from it cause nowadays, namely in international relations. Therefore, cyberterrorism, cyberspace and, consequently, cybersecurity will be analyzed in greater detail and rigor, within the scope of the matter in question.

The time period that will be studied in this dissertation ranges from the first cyber war in 1999, to the Donald Trump elections in 2016, extending to the present day.

It is intended to understand why the change and option for cyberterrorism in recent decades and its impact on international relations today. Given that it is not just about international attacks, but even about legal persons against the state, or other legal entities, it will be opportune to study the various possible and remarkable cases in which such situations occurred.

Keywords: Internet; Cyberterrorism; Cyberspace and Cybersecurity

ÍNDICE

Conteúdo

LISTA ACRÓNIMOS

CIA – Agencia de Inteligência Central

CNU - Carta das Nações Unidas

CTITF – Counter Terrorism Implementation Task Force

DUDH – Declaração Universal dos Direitos Humanos

EUA – Estados Unidos da América

FBI - Federal Bureau of Investigation

#GOP – Guardians of Peace

IAEA – Agência Internacional de Energia Atómica

IDS - Intrusion detection system

IP - Endereço de Protocolo da Internet

IPS - intrusion prevention system

ITRC - Interstate Technology and Regulatory Council

ISIS – Islamic State of Iraq and Syria

NASA – Administração Nacional da Aeronáutica e Espaço

NU – Nações Unidas

ONU – Organização das Nações Unidas

RU – Reino Unido

USSTRATCOM – Comando Estratégico dos Estados Unidos da América

URSS – União Soviética

1. Introdução

Nos dias que correm, o mundo encontra-se cada vez mais interligado através da tecnologia de comunicação e informação do que alguma vez foi possível verificar anteriormente. Os sistemas atuais de telecomunicação e computadores têm um alcance global, transmitindo as nossas vozes, imagens e dados pessoais digitalmente, através de fronteiras transnacionais. Estes sistemas são capazes de suportar infraestruturas económicas, tais como a indústria de energia e transportes aéreos, ou até mesmo todos os tipos de comércio digital e serviços governamentais[1]. Neste momento não existe uma única indústria que não dependa inteiramente da tecnologia e da rede de internet. As vantagens que se podem retirar da internet e do mundo cibernético são imensas, no entanto, toda a vantagem tem um contraponto. Todos os dias dependemos mais e mais de sistemas interconectados como, por exemplo, as telecomunicações, bancos eletrónicos, pagamento de contas e dívidas online, acesso à nossa situação tributária, e a lista continua[2]. Tal como nós, pessoas singulares, também grandes organizações como governos e pessoas coletivas internacionais utilizam estes métodos para aceder aos seus dados pessoais no dia a dia.

Se olharmos para meados do século XX vemos a diferença abrupta no desenvolvimento da comunicação à distância com a invenção da internet. A internet permite o contacto com qualquer pessoa, em qualquer ponto do mundo em tempo real, além de permitir a facilidade de acesso a coisas necessárias do dia a dia. No entanto, quando utilizada em exagero, afeta a forma como como interagimos com outras pessoas, nomeadamente no que toca à criação de armas nucleares, à transformação de vírus digitais em armas mortíferas e, entre tantas outras coisas, também diminui o nível de empregabilidade, retirando postos de trabalho a pessoas e substituindo-as por maquinaria.

O primeiro grande ataque cibernético terrorista de que há registo aconteceu em Janeiro de 2010, mas acredita-se que já tinha sido posto em prática em 2008, demorando

---

[1] Andrew Colarik, *Cyber Terrorism: Political and Economic Implications*, Idea Group Publishing, London, 2015, p. xi.
[2] Ibid..., p. xii.

quase 2 anos a ser descoberto[3]. Em janeiro de 2010, inspetores da Agência Internacional de Energia Atómica enquanto visitavam a fábrica de enriquecimento de urânio de Natanz, no Irão, repararam que as centrífugas usadas para enriquecer o gás com urânio estavam a falhar a uma magnitude sem precedentes, sem causa aparente[4]. Ao mesmo tempo que tentavam solucionar este problema, outros foram aparecendo no mesmo país, até que uma empresa bielorussa foi chamada para tentar descobrir o que estava a causar todos estes fenómenos inexplicáveis[5]. É aqui que se descobre a primeira arma digital do mundo – o vírus, *Stuxnet*.

Embora existam poucas publicações e obras acerca do assunto por ser um fenómeno relativamente recente, os ataques cibernéticos terroristas têm sido cada vez mais recorrentes e, por isso, um assunto de elevada relevância na sociedade atual. O ciberterrorismo apresenta variados problemas aos países e à comunidade internacional, uma vez que tem a capacidade de causar danos virtuais às suas infra-estruturas nacionais, que mais tarde podem vir a tornar-se físicos[6].

Nesta dissertação serão alvo de estudo três grandes problemáticas do mundo cibernético: o fenómeno *Stuxnet*, sobre o qual já foi feita uma introdução, ainda que muito breve; o atentado à liberdade de expressão por parte da Coreia do Norte à empresa americana *Sony*, devido à série cómica *The Interview*; bem como o impacto da atuação da empresa *Cambridge Analytica* face às eleições presidenciais Norte-Americanas e ao *Brexit.* Todos eles têm o mesmo em comum: são ataques cibernéticos. Não se tratam de ataques em pequena escala, mas sim de ataques capazes de roubar informação e dados pessoais, capazes de mudar o destino eleitoral de uma nação, capazes de causar uma guerra nuclear.

A verdade é que, embora seja um problema a cada dia mais comum, continua a não existir legislação internacional específica para combater este fenómeno, deixando as relações internacionais em risco. Cada país, na sua singularidade, adota medidas

---

[3] Wired, An Unprecedented Look at Stuxnet, the World's First Digital Weapon, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[4] Ibidem.

[5] Ibidem.

[6] Pardis Moslemzadeh Tehrani, *Cyberterrorism – The Legal and Enforcement Issues,* World Scientific & Imperial College Press, 2017, London, p. v.

especiais, tais como estatutos, pequenas medidas de cibersegurança, e alguns até se juntaram a certas organizações internacionais com vista a combater este problema. Mas será suficiente para manter uma boa relação entre os estados? Será suficiente para que os nossos dados pessoais e intraestatais estejam protegidos? É essa a resposta que vamos procurar responder nesta dissertação.

Cada vez mais países consideram, além dos espaços terrestre, marítimo e aéreo, também o espaço digital como imprescindível para a segurança da sua população e estado. Patrulhar o espaço digital tornou-se uma das mais prementes tarefas na segurança internacional, tendo em conta que todas as vezes que se abre uma brecha na esfera digital, novos terroristas cibernéticos e formas de ciberterrorismo serão inventadas, violando, novamente, as plataformas governamentais e internacionais. A questão que se coloca é: como é que se pode proteger estas infraestruturas digitais?

Os especialistas parecem concordar que existem duas formas de proteção e defesa face ao ciberterrorismo: defesa ativa e defesa passiva[7]. Defesa passiva trata-se essencialmente de enrijecer a própria esfera de atuação, isto é, consiste no uso de variadas tecnologias e produtos, bem como de processos de proteção da informação e tecnologias utilizadas ou operacionalizadas por um individuo ou organização. Algumas destas formas de defesa passiva podem ser dinâmicas, tais como um ataque ao progresso, mas por definição, uma defesa passiva não traz qualquer risco ou penalidade ao sujeito atacante. Por outro lado, a defesa ativa, por definição, traz enormes riscos e penalidades ao sujeito atacante. Isto significa exposição, investigação, condenação e até mesmo a possibilidade de contra-ataque. Com apenas medidas passivas, os atacantes continuam a usufruir da liberdade de violar a nossa privacidade. Tendo em conta a vulnerabilidade da maioria dos espaços cibernéticos, o baixo custo de grande parte dos ataques, conjuntamente com a habilidade dos atacantes de poder proceder a esses ataques de uma zona segura para os mesmos, torna-se muito mais provável que consigam levar avante os seus planos. Ainda assim é pertinente referir que, por razões de direito internacional público, a maioria das formas de defesa ativa terão sempre de passar por e ficar a cargo dos governos de cada nação[8].

[7] Seymour Goodman, ''Toward a treaty-based international regime on cyber crime and terrorism'', Center for Strategic and International Studies Press, Washington D.C., pp. 65 a 78.
[8] Ibidem.

Em suma, nesta dissertação vamos poder estudar em profundidade o impacto do avanço tecnológico na sociedade atual, bem como todos os problemas advindos desse mesmo avanço. Ser-nos-á possível compreender melhor como funcionam as redes digitais, de que forma apareceram pela primeira vez, como é que podemos usufruir das mesmas com segurança e como é que as podemos proteger em casos de ataques cibernéticos.

Mais importante ainda será o foco no terrorismo digital, ou ciberterrorismo, que se trata de uma ameaça iminente nos dias que correm e para o qual ainda não existe uma solução internacional e global, capaz de parar este tipo de ataque e de proteger não só pessoas singulares, como populações e economias globais.

2. Considerações Conceptuais

2.1. Tecnologia

O termo tecnologia é uma combinação do grego *techne* (arte, artesanato), com *logos* (palavra, discurso), significando, por isso, ‘’um discurso sobre as artes’’[9]. Quando o termo apareceu pela primeira vez como o conhecemos hoje, era apenas usado para se referir a artes aplicáveis, ou seja, arte que era utilizada na decoração e design do nosso dia-a-dia, bem como objetos práticos tornando-os esteticamente apelativos[10]. Mais tarde, no início do século XX, o termo passou a abranger variados meios, processos e ideias, além de ferramentas e maquinaria, levando a que em meados do mesmo século, a palavra tecnologia já fosse usada como ‘’o meio ou a atividade pela qual o homem procura mudar ou manipular o seu ambiente’’[11].

Os seres humanos, ao contrário de outras espécies, não possuem reação instintiva desenvolvida, mas são dotados de algo que as anteriores não: a capacidade de pensar sistemática e criativamente sobre matérias e técnicas complexas, conseguindo, por isso, inovar, modificar, inventar e conservar conscientemente o meio ambiente de uma forma que nenhuma outra espécie alguma vez conseguiu[12]. É aqui que entra, então, o propósito final da tecnologia: a necessidade. Gradualmente e por necessidade, vários engenhos acabaram por ser inventados desde os primeiros tempos do homem na terra, mas a verdadeira revolução tecnológica chegou aquando do século XVIII, na época da Revolução Industrial com a invenção de maquinaria capaz de produzir, pela primeira vez, em massa[13].

2.2. Ciberterrorismo

---

[9] Britannica, *History of Technology,* https://www.britannica.com/technology/history-of-technology.

[10] Oxford Reference, *Applied Arts*, https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095420946.

[11] Britannica, *History of Technology,* https://www.britannica.com/technology/history-of-technology.

[12] DiscoverTec, *The Evolution of Technology: Past, Present and Future,* https://www.discovertec.com/blog/evolution-of-technology.

[13] The Nation, *History and Evolution of Technology,* https://www.nation.com.pk/23-Jul-2018/history-and- evolution-of-technology.

O ciberterrorismo não é completamente diferente do terrorismo ‘’tradicional’’ tal como o conhecemos. De acordo com a doutrina, ‘’terrorismo é um método para inspirar ansiedade através de repetidas ações violentas aplicadas por atores individuais semiclandestinos, por grupos ou Estados, por razões idiossincráticas, criminais ou políticas, através das quais – ao contrário do assassinato – os alvos diretos da violência não são os principais alvos. As vítimas humanas imediatas da violência são geralmente escolhidas aleatoriamente (alvos de oportunidade) ou seletivamente (ou simbólicos alvos) de uma população selecionada, e servem como geradores de mensagens. Ameaça de violência baseada no processo de comunicação entre os terroristas (organização), vítimas (em perigo), e as metas principais são usadas para manipular os principais alvos (audiências) transformando-o num alvo de terror, um alvo de demandas, ou um alvo de atenção, dependendo se o objetivo principal é a intimidação, a coerção, ou a propaganda’’[14].

A definição de ciberterrorismo difere somente no que toca à metodologia aplicada. No ciberterrorismo não existem mísseis, não existem bombas, não existe o envio de tropas ou pessoas para assassinar outras. Existe somente um ataque cibernético a uma plataforma digital que mais tarde poderá vir a resultar num ataque físico, económico e no corrompimento das boas relações interestatais. É nada mais, nada menos, que a convergência entre o espaço cibernético e o terrorismo. É o ataque a computadores, a redes digitais e a toda a informação armazenada nos mesmos para intimidar ou coagir governos, organizações mundiais e estatais a obedecer a certas ideologias politicas ou sociais[15]. Não basta ser um ataque a uma pessoa, tem de ser em grande escala por forma a causar medo a uma nação ou grupo de pessoas, como por exemplo, um ataque digital capaz de causar uma crise económica em larga escala[16].

O ciberterrorismo é a forma perfeita de alcançar fins através de meios mais simples: não há necessidade de ter um exército, de ter armamento e muito menos de ter

[14] Alex P. Schmid, Albert J. Jongman - *Political Terrorism. A guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature*, Amsterdam: North-Holland Publishing Company, 1984, Amsterdão, p. 28.
[15] Gabriel Weimann, Cyberterrorism – How Real is the Threat?, United States Institute of Peace, https://www.usip.org/sites/default/files/sr119.pdf , p. 4.
[16] Ibidem.

um grande orçamento por detrás do ataque[17]. Os agentes por detrás destes ataques aproveitam-se somente da tecnologia e da internet para poder levar a cabo os seus propósitos terroristas, resultando, eventualmente, na possibilidade de haver um ataque capaz de matar milhares e de arruinar economias.

De acordo com Gabriel Weimann[18], o ciberterrorismo torna-se uma opção atrativa para o terrorista moderno por cinco principais razões. Começando pela mais óbvia, Gabriel explica o quão mais barato este tipo de terrorismo é, precisando apenas de um computador e de ligação à internet[19]. Não há necessidade de comprar armamento, precisando apenas de criar um vírus que se dissipe através de ligações telefónicas ou online. Em segundo lugar, explica que o ciberterrorismo é dotado de um anonimato que o terrorismo tradicional não tem[20]. Como terceira razão, aponta o facto da variedade e número de alvos ser muito maior do que a do terrorismo tradicional, ou seja, um terrorista cibernético pode atacar, ao mesmo tempo, variados dipositivos, redes e indivíduos ou pessoas coletivas[21]. Em quarto lugar encontra-se a praticabilidade de poder atacar todos estes dispositivos eletrónicos e consequente informação armazenada à distância[22]. O ciberterrorismo não requer treino físico, não requer investimento psicológico, não implica mortes nem a inconveniência de viajar. Finalmente, aponta para o facto de ter o potencial de atingir um número de pessoas muito mais elevado que o terrorismo tradicional, acabando por gerar, também, muito mais cobertura dos media que, de acordo com Weimann, é o propósito final dos terroristas: causar medo e pânico através dos media[23].

---

[17] Pardis Moslemzadeh Tehrani, *Cyberterrorism – The Legal and Enforcement Issues,* World Scientific & Imperial College Press, 2017, London, p. 2.

[18] Professor de Comunicação no Departamento de Comunicação da Universidade de Haifa em Israel. Estuda os efeitos dos media, campanhas políticas, tecnologia e terrorismo moderno na sociedade atual.

[19] Gabriel Weimann, *Cyberterrorism – How Real is the Threat*?, United States Institute of Peace, https://www.usip.org/sites/default/files/sr119.pdf , p. 6.

[20] Ibidem.

[21] Ibidem.

[22] Ibid..., p. 7.

[23] Ibidem.

CAPÍTULO I

3. A Ameaça do Ciberterrorismo

3.1 A iminência de uma guerra nuclear no Médio Oriente

Em Janeiro de 2002, o então presidente dos EUA, George Bush, fez um discurso no Congresso descrevendo a Coreia do Norte, o Irão e o Iraque como ‘’eixos do mal’’ por quererem desenvolver armas de destruição nuclear[24]. Com este tipo de discurso, as tensões entre os EUA e o Irão aumentavam, colocando em risco o futuro das relações internacionais, vivendo-se um período crítico com a iminência de uma guerra nuclear no Médio Oriente. É então que em Agosto de 2022, um grupo dissidente do Irão, vem divulgar que o governo iraniano estava a enriquecer urânio na sua instalação nuclear em Natanz[25]. A partir daqui deram-se várias tentativas por parte dos EUA de impedir, através de sanções, para travar o Irão, incluindo inspeções regulares por parte da IAEA, para que não acontecesse algum tipo de ataque por parte do Irão. Em Janeiro de 2010, aquando de uma inspeção pela IAEA às centrífugas das fábricas situadas em Natanz, foi descoberta uma falha na capacidade de produção de urânio nunca antes observada. À primeira vista não existia qualquer explicação para o fenómeno, mas cinco meses depois deste primeiro incidente, deu-se outro que nem parecia estar relacionado. Uma empresa de segurança digital foi chamada para tentar arranjar solução para o facto de uma série de computadores, novamente no Irão, estarem a travar e reiniciar repetidamente, impedindo os trabalhadores de os utilizar[26]. É, então, em Setembro de 2010 que se descobre a primeira arma digital do mundo.

3.2. *Stuxnet*: o primeiro ataque ciberterrorista

Ao contrário dos vírus normais, outrora conhecidos, que apenas eram capazes de atacar somente o dispositivo em que eram instalados, este novo vírus, mais tarde

[24] The Economist, *George Bush and the axis of evil*, https://www.economist.com/leaders/2002/01/31/george-bush-and-the-axis-of-evil.
[25] Arms Control Association, *Timeline of Nuclear Diplomacy With Iran*, https://www.armscontrol.org/factsheets/Timeline-of-Nuclear-Diplomacy-With-Iran.
[26] Wired, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon,* https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

denominado de *Stuxnet*, espalhava-se ininterruptamente entre computadores portadores do sistema operacional *Windows*, mesmo entre aqueles que não se encontravam conectados à internet[27], ou seja, bastava que um trabalhador inserisse uma *pen drive USB* num computador infetado, que o vírus era capaz de se infiltrar na mesma e depois espalhar-se no próximo dispositivo em que a *pen* fosse inserida[28]. A facilidade com que o vírus se espalhava levou às piores suspeitas: será que o mesmo proliferou pelo mundo?

Para melhor entender a ameaça que era este vírus, além de perceber como funciona, há que explicar qual era o seu alvo, quem foi o possível criador deste vírus e quais foram os seus efeitos sociais, políticos, económicos e internacionais.

De acordo com os especialistas, o vírus parecia ter sido criado especificamente para atingir a instalação nuclear e de enriquecimento de urânio em Natanz. O que levou a esta conclusão foi o facto de ter sido desenvolvido para atingir dispositivos organizados em grupos de 164 objetos, o mesmo número de centrífugas presentes nas instalações em Natanz[29]. Além disso, o vírus também tinha sido desenvolvido para ser capaz de se espalhar *offline*, novamente coincidindo com o facto de os computadores que controlavam as centrífugas e a própria instalação nuclear, trabalharem somente *offline*[30]. Isto significa que para que o vírus fosse capaz de infetar os computadores nas instalações, alguém o terá colocado numa *pen drive*, que mais tarde veio a ser inserida nos dispositivos em Natanz.

Mas quem é que criou este vírus? De acordo com especialistas em antivírus, devido ao nível de complexidade do *Stuxnet*, era provável que tivesse sido criado por um Estado e não por uma pessoa singular ou grupo independente. Neste caso, tudo apontava para uma cooperação entre os Estados Unidos da América, pelas razões supramencionadas, e Israel, que também teria reiteradamente feito ameaças sancionatórias ao Irão[31]. Em 2012 as suspeitas vieram a ser confirmadas. As autoridades

---

[27] David Kushner, *The Real Story of Stuxnet*, https://courses.cs.duke.edu/spring20/compsci342/netid/readings/cyber/stuxnet-ieee-spectrum.pdf, Duke University, 2013, p. 2.
[28] Ibidem.
[29] Marie Baezner, Patrice Robin, *Stuxnet*, Center for Security Studies, Zurique, 2017, p. 8.
[30] Ibidem.
[31] Ibidem.

americanas, falaram sob condição de anonimato para confirmar que realmente o esforço para travar e danificar gradualmente a capacidade nuclear do Irão, tinha sido desenvolvido pela primeira vez durante o governo de George Bush[32]. A ideia era que fosse uma operação a longo prazo, porque, de acordo com um participante na operação, quando se dá uma destruição imediata, torna-se mais fácil descobrir quem está por detrás da mesma, mas o inverso acontece aquando de uma abordagem mais lenta, levando a que os alvos se sintam incompetentes e culpados[33].

3.3. Efeitos sociais, políticos, económicos e internacionais

Quanto aos efeitos sociais e políticos, a nível nacional, o ciberataque desacreditou o governo Iraniano, que ficou visto como o país que não conseguia proteger as suas próprias instalações nucleares contra a ameaça digital. Isto poderia potencialmente levar a que o governo ficasse mal visto pela população, mas tal não aconteceu. O vírus tinha sido desenvolvido por forma a evitar danos colaterais, isto é, capaz de atacar apenas aquilo para o qual tinha sido desenhado, sem fosse gerada uma onda de violência com perda de vida humana, e impedindo, a curto prazo, tensões acrescidas entre o ocidente e o Médio Oriente[34]. No entanto, e como seria de esperar, o vírus ter-se-á propagado para mais dispositivos ao nível mundial, causando uma sensação de insegurança global, demonstrando o quão simples e assustadora pode ser a invasão da privacidade de cada um de nós. Ainda assim, o ataque também foi capaz de impedir a continuação dos projetos nucleares por parte do Irão, levando a que houvesse um alívio internacional relativamente a essa problemática.

O Irão estava, e continua sujeito a entraves sancionatórios que o impedem de ter acesso aos mercados internacionais para comprar material nuclear, particularmente, no que toca à compra de centrífugas e, portanto, tendo de as construir com material próprio, e componentes que não seriam a escolha primária na sua construção[35]. Somando a isso,

---

[32] The Washington Post, Stuxnet was work of U.S. and Isreali experts, officials say, 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

[33] Ibidem.

[34] Marie Baezner, Patrice Robin, *Stuxnet,* Center for Security Studies, Zurique, 2017, p. 9.

[35] Ibid..., p. 10.

ainda temos a destruição de mais de mil centrífugas aquando do ataque, e a fraca capacidade financeira do país.

A nível internacional não terão havido quaisquer consequências financeiras, uma vez que o Irão, embora esteja a emergir vagarosamente de uma década de estagnação financeira[36], na altura do impacto do ataque, não era, nem de perto, uma potência económica, não tendo, por isso, qualquer impacto financeiro a nível mundial.

A questão mais importante que devemos colocar é: como é que o Stuxnet afetou as relações internacionais? À primeira vista, o ciberataque teve um impacto bastante positivo nas relações internacionais porque, como já foi mencionado, foi capaz de atrasar o enriquecimento de urânio ainda que por um pequeno período de tempo, aliviando as tensões internacionais, e o receio da iminência de uma guerra nuclear no Médio Oriente. No entanto, existem sempre consequências que não eram esperadas e que podem vir a ter um impacto negativo. Neste caso, foi o facto do vírus se ter espalhado a nível mundial. Ter o vírus espalhado, significava que qualquer pessoa poderia alterá-lo e utilizá-lo com a pior das intenções[37]. Havia, agora, a possibilidade de um grupo terrorista usar este vírus para atacar alicerces internacionais. Até aos dias de hoje, que se saiba, não terá acontecido, mas consequentemente, e como forma de proteção interna, os estados começaram a investir em cibersegurança, coisa que anteriormente não era uma prática comum[38].

[36] The World Bank, *Islamic Republic of Iran*, https://www.worldbank.org/en/country/iran/overview.

[37] Marie Baezner, Patrice Robin, *Stuxnet*, Center for Security Studies, Zurique, 2017, p. 11.

[38] Ibidem.

4. A Violação da Liberdade de Expressão Internacional

4.1. Liberdade de opinião e expressão: um direito internacionalmente protegido

Muitas vezes, associamos o terrorismo à religião, especialmente ao islamismo, porque é essa a abordagem que estamos habituados a ver nas notícias que nos chegam. No entanto, e como já foi exposto ao longo desta dissertação, um ataque terrorista não se prende apenas com motivos religiosos, e não é imperativo que para ser considerado como tal, advenha de grupos islâmicos. A definição de terrorismo já supramencionada, é bastante elucidativa no que toca às várias razões do terrorismo, que muitas vezes são desconsideradas pelo facto de, regra geral, as pessoas o associarem somente à religião.

É neste capítulo que vamos explorar um dos (imensos) alvos do ciberterrorismo: os direitos humanos.

A Declaração Universal dos Direitos Humanos foi adotada pela Assembleia Geral das Nações Unidas no dia 10 de dezembro de 1948[39]. Num cenário pós-guerra, tornava-se necessário criar uma base de direito internacional, com a qual todos os países concordassem e fossem capazes de respeitar[40]. A DUDH vem afirmar que os direitos humanos são universais, usufruto de todos, independentemente de quem são ou de onde vivem[41].

A responsabilidade de proteger e fazer respeitar os direitos humanos recai, principalmente, sobre os governos de cada país. Cada governo deve promover os direitos humanos impedindo e proibindo violações aos mesmos, nomeadamente por parte de funcionários e agentes do Estado, processando qualquer um que os infrija, e criando meios, tais como tribunais competentes, independentes e imparciais, para que os cidadãos possam pedir ajuda em casos necessários[42].

No entanto, e como iremos explorar neste sub-capítulo, quando são os próprios governos os responsáveis pela violação de um direito humano, as imposições acima descritas tornam-se inadequadas. Neste último caso, as instituições internacionais, como

[39] Australian Human Rights Commission, *What is the Universal Declaration of Human Rights*?, https://humanrights.gov.au/our-work/what-universal-declaration-human-rights.
[40] Ibidem.
[41] Preâmbulo DUDH.
[42] Human Rights Watch, *What are Human Rights*?, https://www.hrw.org/news/2014/09/15/what-are-human-rights.

o Conselho de Direitos Humanos da Organização das Nações Unidas ou o Comité contra a Tortura têm capacidade limitada para fazer cumprir a lei internacional[43]. Regra geral, os governos que incumpram com a lei dos direitos humanos são apenas responsabilizados publicamente através de organizações não governamentais[44] e através de sanções impostas por outros países, tal como tem acontecido ultimamente com a guerra entre a Rússia e a Ucrânia.

O artigo 19.º da DUDH estabelece que ‘’todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão’’.

4.2. *The Interview:* da sátira ao ciberataque

The Interview foi um filme de comédia, realizado pela empresa *Sony Pictures*, dentro do mesmo género do conhecido *Borat*, com vista a satirizar as idiossincrasias de um país asiático, do ponto de vista ocidental. Originalmente, o alvo da ridicularização era Kim Jong-il[45], mas entre a conceção e a estreia do filme, Kim Jon-il morreu e sucedeu-lhe o seu filho, Kim Jong-un. No dia 11 de junho de 2014, a Sony decide lançar o primeiro trailer do filme no Youtube. O trailer tomava a forma de uma sátira, no qual um apresentador de um programa de televisão em Hollywood e o seu produtor são contratados pela Central Intelligence Agency (CIA), para viajar até à Coreia do Norte e assassinar Kim Jong-un. A mensagem do filme era troçar da cultura de celebridades americana, bem como fazer pouco de toda o mistério que circunda o governo Norte-Coreano.

Logo após a publicação do primeiro trailer, uma carta do embaixador da Coreia do Norte nas NU foi enviada ao Secretário-Geral, dizendo que o filme era absolutamente

[43] Ibidem.
[44] Ibidem.
[45] The Washington Post, *The Sony Pictures hack, explained*, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

intolerável e que a sua distribuição nos EUA se tratava de um ato terrorista e de guerra para deitar abaixo o sistema social da Coreia do Norte[46].

Tanto a Sony, como a Sony Corp. expressaram o seu desconforto para com o polêmico filme, mas ainda assim o CEO da Sony Corp. decidiu exibir o mesmo. [47] A verdade é que, embora sabendo que o filme poderia vir a enfurecer o inimigo, a Sony não teve meias medidas e redefiniu a sua estreia para 25 de dezembro de 2014, após ter feito algumas alterações, tais como o apaziguamento da morte de Kim Jong-un.[48]

Na segunda-feira anterior ao *Thanksgiving* ou, em português, dia de Ação de Graças, os trabalhadores da Sony Pictures que tentaram entrar nos seus computadores, foram presenteados com um gráfico de um esqueleto vermelho, com as palavras ‘’#Hacked by #GOP’’, e uma ameaça de expor informação privada da empresa, caso um certo pedido, não especificado, não fosse cumprido[49]. O problema que se levantava, é que não era apenas uma ameaça, mas também uma tática já posta em prática, uma vez que os *links* que apareciam na faixa inferior do ecrã levavam a listas de documentos e ficheiros da Sony que a #GOP dizia ter roubado da empresa, bem como emails para que os trabalhadores da Sony pudessem contactar os membros da #GOP e responder aos pedidos que faziam.[50]

Todos os dias saíam notícias que apontavam deficiências no sistema de segurança cibernética da Sony. Outrora já se tinham dado inúmeros ataques cibernéticos na rede da Sony Playstation, a qual desenvolveu uma rede de segurança muito mais forte e coesa, mas, infelizmente, a Sony não adotou o mesmo sistema.[51] O problema da Sony não era apenas online, era também físico, já que no dia 3 de novembro do mesmo ano, aquando de uma reunião entre os diretores executivos da Sony e outra empresa, a última relatou ser extremamente fácil entrar no desprotegido e destrancado escritório de segurança de

---

[46] Nações Unidas, Assembleia Geral do Conselho de Segurança, ‘*’Letter dated 27 June 2014 from the Permanent Representative of the Democratic People’s Republic of Korea to the United Nations Addressed to the Secretary-Gerenal’’*, A/68/934-S/2014/451, 27 de junho de 2014.

[47] Vanity Fair, *An Exclusive Look at Sony’s Hacking Saga*, março 2015, https://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.

[48] Fortune, *Inside the Hack of the Century. Part 2: The Storm Builds*, junho 2015, https://www.fortune.com/sony-hack-part-two/.

[49] The Washington Post, *The Sony Pictures hack, explained*, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

[50] Antonio DeSimone, Nicholas Horton, *Sony’s Nightmare Before Christmas,* The Johns Hopkins University Applied Physics Laboratory, 2017, p. 14.

[51] Ibid..., p. 15.

informação, tendo acesso a computadores igualmente desprotegidos, que armazenavam informação da rede internacional da Sony.[52]

Mas como é que a #GOP conseguiu ter acesso a toda esta informação e entrar na rede da Sony? A resposta é simples, e provavelmente qualquer pessoa que esteja a ler esta dissertação já passou por uma situação semelhante.

De acordo com a análise pós-ataque do FBI, conclui-se que a primeira violação da rede da Sony deu-se em setembro de 2014, meses antes da ameaça feita pela #GOP. Os hackers entraram na rede através do envio de e-mails falsos, comumente conhecidos como *phishing*, para os trabalhadores da Sony, nos quais estariam links para websites falsos, acompanhados de mensagens que diziam que os trabalhadores perderam acesso á plataforma x da Sony, tendo, por isso, de colocar as suas credenciais novamente para voltar a ter acesso à mesma.[53]

Roubar informação não era o único objetivo da #GOP, os vírus instalados nos computadores e nas redes digitais eram capazes de estragar o disco rígido[54] dos mesmos, ao ponto de nem serem capazes de os ligar novamente.[55]

Figura 1. Imagem apresentada num monitor de um computador da Sony a 4 de novembro de 2014 (Imgur)

[52] Ibidem.

[53] Ibid..., p. 16.

[54] Uma unidade de disco é um dispositivo que lê e/ou grava dados em um disco. O tipo mais comum de unidade de disco é um disco rígido (ou "unidade de disco rígido"), mas também existem vários outros tipos de unidades de disco. Alguns exemplos incluem dispositivos de armazenamento removíveis, unidades de disquete e unidades ópticas, que lêem mídia óptica, como CDs e DVDs.

[55] Antonio DeSimone, Nicholas Horton, *Sony's Nightmare Before Christmas,* The Johns Hopkins University Applied Physics Laboratory, 2017, p. 16.

A Sony desconectou a sua rede digital da internet assim que chegou à conclusão de que estava comprometida. No entanto já era demasiado tarde para isso, uma vez que milhares de computadores e servidores online já se encontravam inutilizáveis, obrigando a empresa a debruçar a sua confiança apenas em dispositivos que nunca tinham sido comprometidos anteriormente, pondo de parte tudo o que eram smartphones, computadores, entre outros, e voltando a usar os antigos Blackberries, arquivos em papel e reuniões presenciais, ao invés de online.[56]

Enquanto a Sony lutava para impedir a continuação da violação de informação, a #GOP continuava a expor informação da mesma, tal como filmes por estrear, guiões de filmes que ainda nem tinham começado a ser filmados, números de segurança social e identificação fiscal dos trabalhadores, etc.[57]

4.3. O anonimato nos ciberataques

O problema que se levanta com todos os ciberataques é o mesmo: quem foi o verdadeiro cérebro por detrás da ação? Ao contrário do terrorismo tradicional como o conhecemos, o cibeterrorismo é dotado de anonimato. Não é necessário ‘’dar a cara’’ para que se possa roubar dados, informação, deitar abaixo websites e bolsas on-line. A única forma de descobrir quem são os verdadeiros agentes por detrás de um ataque ciberterrorista é utilizando a mesma ferramenta de trabalho que eles: a internet.

Aquando do ataque, e para tentar descobrir quem estaria por detrás do mesmo, a Sony contratou a empresa Mandiant, que faz parte da multinacional FireEye.[58] Ao mesmo tempo que a Mandiant estudava o caso, outras empresas, por conta própria, e por beneficiarem mais tarde do caso, na eventualidade de descobrirem primeiro quem era o cérebro da operação, começaram a investigar também. Foi através de uma dessas empresas que se apontou o dedo pela primeira vez à Coreia do Norte, na primeira semana de Dezembro.[59] Os especialistas pareciam ter chegado à conclusão que os ataques eram provenientes da Coreia do Norte, uma vez que tinha havido um com muitas semelhanças

---

[56] Ibidem.
[57] Ibid..., p. 17.
[58] Reuters, Sony *Hires Mandiant after cyber attack, FBI starts probe*, www.reuters.com/article/us-sony-cybersecurity-mandiant/sony-hires-mandiant-after-cyber-attack-fbi-starts-probe-idUSKCN0JE0YA20141201.
[59] Business Insider, *Experts: The Sony Hack Looks a Lot Like Previous Attacks on South Korea*, www.businessinsider.com/experts-say-sony-hack-looks-a-lot-like-previous-attacks-on-south-korea-2014-12.

em março de 2013 contra a Coreia do Sul, o qual foi capaz de danificar as redes digitais dos sistemas financeiros e televisivos da Coreia do Sul.[60]. Ainda assim, havia quem defendesse o contrário e achasse que era ‘’estranho’’ a Coreia do Norte atacar uma potência como os EUA por causa de um filme, quando existem tantos outros do mesmo género.[61]

Em 2015, o Presidente dos EUA, Barack Obama, decidiu retaliar contra a Coreia do Norte através de sanções financeiras.[62] O porquê desta escolha está ligado ao que foi exposto no inicio deste sub-capítulo no que toca à violação dos direitos humanos por parte de governos. Neste caso deu-se a violação da liberdade de expressão de uma empresa multinacional, com origem nos EUA. Esta empresa representa o artigo 19.º, que expressa que não existem limites à liberdade de expressão, e muito menos, a meu ver, quando se trata de uma sátira num filme, como existe com tantos outros países. Como supra-mencionado, ao haver uma violação por parte de um governo a um direito internacional, a única forma de repreender esse governo é através de sanções financeiras e económicas a esse país, já que não existem meios físicos de repreensão.

Além disso, é também importante frisar que a Coreia do Norte nunca chegou a assumir qualquer ataque da sua parte contra a empresa, afirmando apenas que tinha sido merecido porque realmente era uma peça de mau gosto contra o sistema norte-coreano[63], tendo sido um ato consciente, da parte de Obama, não retaliar digitalmente, mas apenas através de sanções, já que embora não houvesse confirmação de que teria sido o governo norte-coreano, o ataque tinha, de facto, provindo de um grupo terrorista norte-coreano[64].

5. *Cambridge Analytica* – as presidenciais Norte-Americanas de 2016

[60] David M. Martin, *Tracing the Lineage of DarkSeoul,* SANS Institute, 2016, https://www.sans.org/reading-room/whitepapers/critical/tracing-lineage-darkseoul-36787

[61] Business Insider, *Experts: The Sony Hack Looks a Lot Like Previous Attacks on South Korea,* www.businessinsider.com/experts-say-sony-hack-looks-a-lot-like-previous-attacks-on-south-korea-2014-12.

[62] New York Times, *More Sanctions on North Korea after Sony Case,* https://www.nytimes.com/2015/01/03/us/in-response-to-sony-hack/2014/12/22/b76fa0a0-8a1d-11e4-9e8d-0c687bc18da4_story.html.

[63] The Washington Post, *The Sony Pictures hack, explained*, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

[64] Deadline, *The Sony Hack One Year Later: Just Who Are The Guardians of Peace?,* https://deadline.com/2015/11/sony-hack-guardians-of-peace-one-year-anniversary-1201636491/.

5.1. Dados pessoais e de utilizador

Para melhor aprofundar esta matéria, e antes de expormos o caso da *Cambridge Analytica,* será pertinente questionarmo-nos sobre o que são dados pessoais.

De acordo com o *website* oficial da Comissão Europeia, dados pessoais são qualquer informação que se relaciona com um individuo vivo, identificado ou identificável, ou, ainda, quaisquer informações que, analisadas conjuntamente, possam levar à identificação de uma determinada pessoa[65]. São exemplos de dados pessoais o nome de uma pessoa singular, a morada, o número do documento de identificação, entre outros.

Assim, e como forma de proteger esses dados, existem pelo mundo variados regimes de proteção de dados. Em Portugal, é aplicável o Regulamento (UE) 2016/679, ou Regulamento Geral sobre a Proteção de Dados da União Europeia, que ‘’estabelece as regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas na UE’’[66]. É importante ressalvar que o Regulamento Geral sobre Proteção de Dados não é aplicável a pessoas falecidas, entidades e pessoas coletivas e, ainda, a pessoas singulares que exerça atividades que nenhuma ligação tenham com atividade comercial e profissional[67].

Quando nos inscrevemos no *Facebook*, no *Instagram*, no *Twitter* ou em qualquer outra rede social, ou aplicação, damos acesso aos seus criadores e bases de dados para armazenar informação sobre nós. Inserimos o nosso nome, a nossa idade, damos **acesso à nossa localização** quase sem nos apercebermos, bem como a que a aplicação utilize o seu algoritmo para **controlar cada movimento que façamos dentro do *website***. A isto chamamos ‘’**user data**’’ ou, em português, dados do utilizador[68]. Os dados do utilizador permitem às empresas, donas destes *websites*, traçar um perfil de cada um de nós, baseado nas nossas preferências de conteúdo conforme assistimos e reagimos nas suas

---

[65] European Comission, *What is personal data,* https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en.

[66] Secretaria-Geral da Presidência do Conselho de Ministros, *Regulamento Geral de Proteção de Dados,* https://www.sg.pcm.gov.pt/sobre-nos/regulamento-geral-de-prote%C3%A7%C3%A3o-de-dados.aspx.

[67] Your Europe, *A proteção de dados ao abrigo do RGPD,* https://europa.eu/youreurope/business/dealing- with-customers/data-protection/data-protection-gdpr/index_pt.htm#shortcut-1,.

[68] Internal Results, *The Complete Guide to Content Personalization,* https://www.internalresults.com/resources/content-personalization.

plataformas, o tempo que passamos a vê-lo, o número de horas que passamos dentro da aplicação, entre tantos outros fatores. A consequência do traçar desse perfil, é que a partir daí, as empresas conseguem **manipular tudo aquilo que vemos** e que conteúdos consumimos.

5.2. Cambridge Analytica e as eleições presidenciais norte-americanas

‘’*While techonology has enabled more sophisticated ways for partisans to manipulate the electorate, it alone isn’t the problema; to find the real source, we must look deep within ourselves’’*[69].

A 8 de novembro de 2016, Donald Trump ganhou, oficialmente, as eleições nacionais nos Estados Unidos, tomando posse no dia 20 de Janeiro de 2017[70]. Para muitos isto significou o fim de uma era de prosperidade e paz para os Estados Unidos, para outros significou o início de uma nova fase que há muito esperavam. Consigo trouxe uma ideologia radicalmente diferente, e uma promessa de derrubar décadas de costume, prática e política externa dos Estados Unidos[71]. Trump também demonstrava uma grande intolerância racial e religiosa, bem como desrespeito pelo tema das alterações climáticas, tema esse que dizia ser falso porque acreditava não existirem. Mas como é que uma pessoa tão problemática consegue ganhar, tão facilmente, as eleições de um país que se identifica pela liberdade e prosperidade? É aqui que iniciamos a exposição do escândalo da empresa ***Cambridge Analytica***.

Criada em 2013, a ***Cambridge Analytica*** é uma empresa britânica, com sede em Londres, que oferece serviços a empresas e partidos políticos que pretendem ‘’mudar o comportamento do público’’[72]. O método de trabalho da mesma passa por analisar grandes quantidades de dados dos consumidores, e combiná-los com a ciência comportamental para identificar pessoas que as organizações podem atingir através de

---

[69] Hal Berghel, *Malice Domestic: The Cambridge Analytica Dystopia,* University of Nevada, Las Vegas, 2018, p.84.
[70] Laetitia Langlois, OpenEdition Journals, *Trump, Brexit and the Transatlantic Relationship: The New Paradigms of Trump Era,* https://www.journals.openedition.org/lisa/10235, 2018.
[71] Dina Parjis, Jeremy Shapiro, European Council on Foreign Relations, *The transatlantic meaning of Donald Trump: a US-EU Power Audit, https://ecfr.eu/publication/the_transatlantic_meaning_of_donald_trump_a_us_eu_power_audit7229/,21,* 21 de setembro, 2017.
[72] The Guardian, *What is Cambridge Analytica?,* https://www.theguardian.com/news/2018/mar/18/what- is-cambridge-analytica-firm-at-centre-of-facebook-data-breach.

marketing digital. Esses dados são recolhidos de uma panóplia de fontes, incluindo plataformas digitais, tais como o ***Facebook***[73].

A história da *Cambridge Analytica* começa em 2014, quando o cientista de dados *Aleksandr Kogan*, entre outros relacionados com a Universidade de Cambridge, criaram uma empresa chamada ‘’Global Science Research’’ para comercializar uma nova aplicação da antiga *Facebook*, chamada ‘*’thisisyourdigitalife’’,* que recolhia informação pessoal dos 50 milhões de participantes que faziam um teste de personalidade, usufruindo dessa mesma informação para fins políticos[74]. O problema não acabou aí, mas sim no facto de além de terem acesso às respostas do teste, também ganharam acesso total às contas de *Facebook* das pessoas que nele participaram e de todos os seus amigos[75]. Mais tarde, toda essa informação foi utilizada pela consultora política, *Cambridge Analytica*, que trabalhava com o partido Republicano desde 2013 e, alegadamente, desempenhou um forte papel na eleição de Trump em 2016[76].

Desde sempre que existiram formas de manipular os votos dos cidadãos nas eleições, ainda mais, em grandes países como os Estados Unidos e a Rússia, por exemplo. Entre essas formas estão o partidarismo, o discurso chocante e populista, e a adulteração de votos. No entanto, aquilo que, na minha opinião, distingue a eleição de Trump das restantes, é o uso de informação e dados pessoais para manipular os eleitores através de anúncios e conteúdo direcionado nas redes sociais[77].

Em 2018, a *Facebook* admitiu terem sido recolhidos dados, indevidamente, pela empresa *Cambridge Analytica*, empressa essa que até hoje nega ter utilizado qualquer uma dessas informações para ajudar na campanha política dos Republicanos em 2016[78].

Mas a verdadeira questão que se coloca aqui é: como é que se manipula a mente de um eleitor? Como é que se transformam cliques no computador em votos? Como é que um anúncio ou conteúdo digital leva a que deixe de votar no partido x para passar a votar no y?

---

[73] ibidem.

[74] L. Ashworth, T. Gillespie, *Who is Dr. Aleksandr Kogan, the Cambridge Academic Accused of Misusing Facebook Data?’’,* Varsity, www.varsity.co.uk/news/15192.

[75] S. Vaughan-Nichols, *How Cambridge Analytica used your Facebook Data to help elect Trump,* Networking, https://www.zdnet.com/article/how-cambridge-analytica-used-your-facebook-data-to-help- elect-trump/.

[76] T.B. Lee, *Facebook’s Cambridge Analytica Scandal, Explained,* Technica, www.arstechnica.com/tech-policy/2018/03/facebooks-cambridge-analytica-scandal-explained.

[77] S. Vaughan-Nichols, *How Cambridge Analytica used your Facebook Data to help elect Trump,* Networking, https://www.zdnet.com/article/how-cambridge-analytica-used-your-facebook-data-to-help- elect-trump/.

[78] Ibidem.

De acordo com Christopher Wylie, um antigo trabalhador da Cambridge Analytica, que também teve o seu papel na criação da tal aplicação para recolher dados pessoais, primeiro é preciso compreender a ciência de dados pessoais, através do estudo da psicologia humana e de como funcionam as ‘*’bored rich women’’*.[79] O primeiro passo, de acordo com o mesmo, é criar uma espécie de treino ou teste, antes de ser criado um algoritmo. Isto é, independentemente do tipo de informação que queremos recolher, não vale a pena traçar o perfil de alguém simplesmente baseando-nos nos ‘’gostos’’ que a pessoa faz, mas sim fazer um teste ao qual a pessoa responde, com uma certa percentagem de honestidade, acerca da sua personalidade.[80] Daí ter sido criada a aplicação que o permitiu em 2015. Por outro lado, é necessário também que hajam as variáveis previsíveis, ou seja, aquilo que a empresa quer prever com base nas nossas personalidades, ou orientações políticas, por exemplo.[81] As 120 questões que se colocavam nesta aplicação provinham de cinco variáveis: o quão aberta a pessoa estava a novas experiências, o quão consciente ela estava no que toca a certos problemas atuais, o quão extrovertida a pessoa é, o quão facilmente ela aceita certas imposições e, finalmente, a sua empatia social.[82]

Mas como é que conseguimos que milhares de pessoas tenham tempo e queiram fazer um teste de 120 questões? A resposta de Wylie era simples: dinheiro. De acordo com Wylie no seu livro ‘’Mindf*ck’’, para algumas pessoas, o incentivo para preencher um formulário ou fazer um teste é financeiro. Isto é, se se tratar de um estudante ou alguém que simplesmente gostaria de fazer uns 5$ a mais, o facto da aplicação dizer que lhes paga para preencher o formulário, já é incentivo suficiente. Wylie explica que os maiores incentivos financeiros iam para os grupos menos fáceis de manipular, ou seja, o grupo menos suscetível de preencher o formulário, e que ganharia mais com isso. Neste caso, foram os homens de ascendência Afro-Americana.[83] Além destes, também foram utilizados outros utilizadores tais como senhoras ricas e mais velhas, que passam os seus

---

[79] Alex Hern, *Cambridge Analytica: how did it turn clicks into votes?,* The Guardian, https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes- christopher-wylie.

[80] Ibidem.

[81] Ibidem.

[82] Ibidem.

[83] Christopher Wylie, *Mindf*ck – Inside Cambridge Analytica's Plot to Break the World,* Reino Unido, 2019, Profile Books, pp. 76 a 78.

dias nos Hamptons *''and end up taking the survey because what do you do when you're alone and old in the Hamptons?''*.[84]

O mecanismo utilizado pela *Cambridge Analytica* era tanto ao quanto simples. Combinado com a recolha destas 120 respostas estava, também, a notificação de acesso ao perfil de *Facebook* desses utilizadores, que dizia que a aplicação teria acesso a todos os seus dados desde que o utilizador assim o aceitasse. É claro que, tal como todos nós, esses milhares de utilizadores que instalaram a aplicação e queriam, ou passar tempo, ou receber um extra de dinheiro, aceitaram os termos e condições mal lhes apareceram na frente, sem que tirassem 5 minutos do seu dia para os lerem. Foi assim que toda a sua informação e, consequentemente de todos os amigos que tinham na plataforma *Facebook* passaram a ser propriedade, também, da *Cambridge Analytica*[85].

Wylie explica ainda que foram criados 253 algoritmos, capazes de gerar 253 previsões por cada utilizador cuja informação tivesse sido recolhida, levando a que o objetivo principal tivesse sido atingido: foi feito um mecanismo que era capaz de pegar nos ''gostos'' que todos os utilizadores norte-americanos faziam no Facebook, e trabalhar ao contrário. Isto é, um mecanismo capaz de preencher as lacunas quanto à personalidade de utilizadores que nunca tinham sequer preenchido o formulário, mas que pela amostra daqueles que o tinham feito, eram também manipulados através do conteúdo e anúncios que a plataforma digital lhes mostrava.[86] Assim, cada utilizador com base naquelas cinco variáveis supramencionadas teria anúncios diferentes conforme o tipo de variável em que se inseria. Um ótimo exemplo para explicar como este algoritmo funciona é o tema da saúde. Qualquer político sabe que a saúde é um tópico de extrema importância na sua campanha, no entanto, é necessário haver um discurso que o distinga dos restantes e que não seja neutro e trivial. É aqui que entra o algoritmo das cinco variáveis. Quando o Facebook mostra aos utilizadores um anúncio de campanha sobre a saúde, irá fazê-lo com base na variável que mais se adequa à pessoa em especifico. Isto é, se me considero uma pessoa conservadora, o anúncio dirá, por exemplo, que o político x não concorda com a eutanásia, se me considero uma pessoa liberal, então já dirá que, por outro lado, este politico concorda com o aborto até às dez semanas, e por aí em diante.[87]

---

[84] Ibidem.

[85] Alex Hern, *Cambridge Analytica: how did it turn clicks into votes?,* The Guardian, https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes- christopher-wylie.

[86] Ibidem.

[87] Ibidem.

Todos os anúncios e conteúdos digitais mostrados no *Facebook*, eram especificamente engendrados para, alegadamente, manipular a perceção dos eleitores, para que votassem no candidato Trump, enfatizando essa manipulação naqueles que eram de mais fácil coação: os menos abastados, eleitores de estados interiores e com menos escolaridade, portadores de deficiência ou fragilidade social, entre tantos outros. E foi assim que Trump conseguiu um grande avanço nas eleições em 2016.

5.3. O impacto no panorama internacional

Como é que a manipulação de votos e utilização de meios digitais afeta o panorama internacional?

Desde já, a eleição em si, utilização ilegal de dados pessoais à parte, mudou completamente o mundo das relações internacionais. Desde o início da campanha que Trump sempre defendeu o ideal de ''América em primeiro lugar'', algo muito mal visto aos olhos do mundo, já que um dos ideais base das relações Transatlânticas e internacionais é a igualdade estatal e cooperação, pondo em causa a segurança do próprio panorama internacional.[88] Além disso, Trump ''abanou'' os alicerces da NATO mais do que qualquer um dos seus antecessores, mesmo aqueles em efeitividade de funções. Referiu inúmeras vezes, em vários dos seus discursos, durante, e antes da tomada de posse, que a NATO era uma organização obsoleta e que de nada servia para combater o terrorismo, causando perplexidade nas capitais europeias, tendo em conta o envolvimento da mesma durante 15 anos no Afeganistão.[89]

Ainda assim, os mais graves acontecimentos deram-se aquando da sua tomada de posse. Trump decidiu retirar os Estados Unidos do Acordo de Paris, anunciando, no dia 1 de junho de 2017 que enquanto iria retirar o país do acordo, também iria iniciar negociações para alterar os termos do mesmo, de modo a que favorecessem os Estados

---

[88] Dina Parjis, Jeremy Shapiro, European Council on Foreign Relations, *The transatlantic meaning of Donald Trump: a US-EU Power Audit, https://ecfr.eu/publication/the_transatlantic_meaning_of_donald_trump_a_us_eu_power_audit7229/,21,* 21 de setembro, 2017.

[89] Fabrice Pothier, Alexander Vershbow, *NATO and Trump The Case for a New Transatlantic Bargain,* Atlantic Council, Brent Scowcroft Center on International Security, https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/NATO_and_Trump_web_0623.pdf, p. 1.

Unidos e os seus contribuintes.[90] A saída americana do Acordo de Paris também veio a significar o fim das contribuições dos Estados Unidos para um fundo global de ajuda aos países de menor dimensão e mais pobres, que arcam com os custos desproporcionais das alterações climáticas.

Trump decidiu, também, retirar os Estados Unidos do Acordo Nuclear com o Irão, indo contra a política externa defendida por Barack Obama e isolando o país dos seus aliados ocidentais, deixando no ar falta de segurança e incerteza relativamente às intenções do presidente.[91]

Finalmente e, a meu ver, a mais chocante iniciativa de Trump, foi a saída da Organização Mundial da Saúde. A 14 de abril de 2020, quando ficou claro que a Covid-19 se tinha infiltrado na população dos Estados Unidos, Donald Trump alegou numa conferencia de imprensa que a disseminação do vírus no país era culpa da OMS e não da sua administração.[92] Algumas semanas depois, em meados de Maio, escreveu uma carta ao Diretor Geral da OMS na qual fazia alegações falaciosas acerca dos esforços da organização nos primeiros dias de aparecimento da doença.[93] A 29 de Maio de 2020, Donald Trump anunciou publicamente que iria cortar relações com a organização. A 6 de Julho de 2020 a administração americana notificou oficialmente o Secretário Geral das Nações Unidas, Engenheiro António Guterres, da sua intenção de abdicar do lugar na OMS.[94]

O panorama internacional mudou abruptamente com a chegada de Trump ao poder, levando a que fosse criado um ambiente de instabilidade e falta de confiança nas relações internacionais.

A tecnologia e o digital têm um poder imenso que, quando em mãos erradas, pode levar a situações extremas e perigosas para as relações internacionais. É por isso que é de extrema importância estudar como funcionam as plataformas digitais, saber lidar com

---

[90] White House, 1 de Junho de 2017, *Statement by President Trump on The Paris Climate Accord* https://www.whitehouse.gov/briefings-statements/statement-president-trump-paris-climate-accord/.

[91] Kali Robinsons, Council on Foreign Relations, 25 de fevereiro de 2021, *What is the Iran Nuclear Deal?,* https://www.cfr.org/backgrounder/what-iran-nuclear-deal.

[92] WhiteHouse, 14 de Abril de 2020, *Remarks by President Trump in Press Briefing,* https://www.whitehouse.gov/briefings-statements/remarks-president-trump-press-briefing/.

[93] FactCheck, 15 de Abril de 2020, *FactChecking Trump's Attack on the WHO,* https://www.factcheck.org/2020/04/factchecking-trumps-attack-on-the-who/.

[94] Ibidem.

elas e ter atenção àquilo que permitimos que elas tenham acesso diariamente. Tudo aquilo que colocamos na internet uma vez, fica para sempre nela guardado.

O escândalo da *Cambridge Analytica* é a prova concreta de que a internet pode ser um lugar muito perigoso aquando da manipulação do panorama internacional. Em momento algum se pensou que Donald Trump iria ganhar as eleições contra Hillary Clinton.

Se foi possível manipular eleições e alterar a consciência dos eleitores através do meio digital, o que mais não será possível fazer? Estaremos nós perante uma ameaça eminente de uma guerra cibernética? Perante uma possível terceira guerra mundial, fruto de segredos de estado que são deitados cá para fora por *hackers*?

CAPÍTULO II

6. Os EUA: uma força cibernética

6.1. Ciberpoder

Para melhor compreender o porquê dos EUA serem considerados uma força cibernética e dotados de um enorme ciberpoder, é necessário explorar o conceito por detrás do mesmo.

O conceito de ‘’poder’’ tradicional – ‘’a habilidade ou direito de controlar pessoas ou coisas’’[95] – não é novo, e ainda que existam inúmeras definições para o mesmo, a que nos interessa aqui é a que se encontra relacionada com o poder nas relações internacionais, nomeadamente no que toca ao ciberpoder e como este afeta as relações entre países nos dias que correm.

Embora haja um acordo generalizado de que o poder é algo muito importante, não significa que haja consenso quanto à definição de poder, nem quanto a termos relacionados, tais como controlo, influência, persuasão, autoridade e coação.[96] Desde 1957 com a obra ‘’The Concept of Power’’ de Robert A. Dahl que é reconhecida a falta de coesão no que toca a uma definição de poder.[97] Mas é com Kaplan que começa a haver uma revolução no conceito, capaz de o definir através de 4 variações: primeiro, de que poder é um conceito casual; segundo, que o poder deve ser visto como um conceito relacionável, ao invés de um conceito próprio; terceiro, que poder é um conceito multidimensional; e quarto, que as bases de poder são muitas, sem uma hierarquia especifica entre elas.[98]

---

[95] The Britannica Dictionary – power.

[96] David A. Baldwin, *Power and International Relations: A Conceptual Approach,* Copyright 2016, Princeton University Press, Estados Unidos, p. 2.

[97] Ibidem.

[98] Ibid..., p. 3.

O poder cibernético repousa sobre um conjunto de recursos que se relacionam com a criação, controle e comunicação de informações eletrónicas através do computador – intraestruturas, redes, software, etc.[99] Isso, claro está, inclui computadores conectados através de uma rede comum, mas também intranets, tecnologias celulares e de comunicação.[100]

Se definirmos comportamentalmente o poder cibernético, ele é nada mais que a habilidade de atingir certos objetivos através da informação digital interconectada dentro do ciberespaço.[101] Já o ciberespaço, por definição, é um domínio operacional enquadrado pelo uso da eletrónica para explorar informações através de sistemas interconectados e as suas respetivas infraestruturas.[102]

O que se torna mais interessante no que toca ao poder cibernético, é o facto de ser representado por um vasto número de atores e não apenas por aqueles que pensaríamos serem os ‘’típicos’’ poderosos como, por exemplo, no mundo financeiro. No mundo cibernético, qualquer um pode ter um enorme poder desde que saiba trabalhar e usar os recursos digitais corretamente. Qualquer um, desde organizações mundiais e governos, até a um adolescente que aprender a arte de hacking, pode causar danos no ciberespaço, e esconder que o fez por detrás do benefício do anonimato que o mundo digital oferece.

6.2. Os primeiros passos para a cibersegurança

Com o passar dos anos, a maioria dos governos chegou à conclusão de que já não bastava ter um bom exército fisicamente, mas era necessário começar a apostar numa espécie de ‘’exército cibernético’’ que fosse capaz de proteger, também, as infraestruturas digitais do seu país.

O reconhecimento da necessidade de segurança e defesa do mundo tecnológico nos EUA começou nos anos 70, quando em 1972 foram feitos esforços de inteligência militar para reduzir a vulnerabilidade e proteger os sistemas de informação.[103] A partir

---

[99] Joseph S. Nye, Jr., Cyber Power, Harvard Kennedy School, Maio 2010, https://apps.dtic.mil/sti/pdfs/ADA522626.pdf, p. 3.
[100] Ibidem.
[101] Ibid..., p.4.
[102] Ibid..., p. 3.
[103] U.S. Cyber Command, *Our History*, https://www.cybercom.mil/About/History/.

das décadas de 80 e 90, começaram a aparecer os primeiros indícios daquilo que um dia viria a ser chamado de *hacking*, tentativas de ciberespionagem, chegando a reconhecer, em 1995, que as forças militares dos EUA eram suscetíveis a ataques remotos, através das redes digitais.[104]

A 23 de junho de 2009, o então Secretário de Defesa do Comando Estratégico dos EUA, dirigiu a criação do Comando Cibernético dos EUA através de um memorando, já que reconhecia a crescente importância e vulnerabilidade dos computadores e redes digitais nos EUA e em todo o mundo.[105] A era da informação e tecnologia estava rapidamente a mudar o mundo e a forma como funcionava, criando redes globais e permitindo que adversários acedessem a centros estratégicos de poder nacional, através da internet. O USCYBERCOM continua a funcionar nos dias de hoje e é composto por quatro entidades: o Comando Cibernético do Exército dos EUA (ARCYBER), o Comando Cibernético da Força Aérea dos EUA (AFCYBER), o Comando Cibernético da Marinha (MARFORCYBER), e o Comando Cibernético das Frotas (FLTCYBER).

De acordo com os especialistas, os EUA são o único país com forte presença global em usos civis e militares do ciberespaço, embora essa presença seja seriamente ameaçada pela China e pela Rússia nos tempos que correm.[106] Em resposta, o governo americano está a adotar uma abordagem robusta e urgente para ampliar as suas capacidades nas operações cibernéticas, tanto para a segurança de sistemas nacionais, como para ampliar as suas ambições no exterior na esfera diplomática, política, económica e militar.[107] Os EUA são dotados de uma superioridade extraordinária face a todos os outros países em termos de tecnologias de informação e comunicação, ainda assim há que ter em atenção que esta não é uma posição de monopólio, havendo sempre possibilidade de aparecer quem tenha mais e melhor.

Os EUA têm uma panóplia de estratégias nacionais para a defesa e segurança no ciberespaço que vêm sido amadurecidas ao longo dos últimos 30 anos. Existem três grandes domínios: defesa da nação, conflitos de baixa intensidade e guerras de alta

---

104 ibidem.
105 ibidem.
106 IISS, *CyberPower – Tier One*, https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-one.
107 IISS, *Cyber Capabilities and National Power: A Net Assessment, Research Papers*, 28 de junho de 2021, https://www.iiss.org/-/media/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---united-states.pdf, p. 15.

intensidade.[108] A preocupação principal tem sido preencher as lacunas que resultaram da exposição de segredos de Estado, roubo de propriedade intelectual, interferência estrangeira através do ciberespaço na política dos EUA e ainda o fraco empenho de segurança cibernética de muitos setores económicos e sociais.[109]

Nos últimos anos, e com a melhoria do ciberespaço e ciberpoder da Rússia e China, tem sido cada vez mais difícil a manutenção da posição dos EUA no que toca à sua cibersegurança. As empresas americanas e o próprio governo têm sido atacadas por nações muito menos capazes, incluindo não apenas os dois países citados anteriormente, mas também pelo Irão e Coreia do Norte, como já vimos no capítulo anterior. O problema que se coloca é que os hackers do governo americano são menos propensos a ripostar de igual forma, porque estão a tentar seguir as ‘’regras de bom comportamento’’ no ciberespaço que pelo contrário os seus adversários ignoram.[110]

A maior diferença entre os EUA, e os seus aliados (Reino Unido, França, e Austrália) e a China e a Rússia, é que enquanto os primeiros apostam mais na tecnologia de cibersegurança, os segundos apostam na tecnologia de ciberataques. Ou seja, embora a Rússia e a China tenham maior capacidade de ataque e hacking, os EUA e os aliados têm uma muito superior capacidade de proteção e segurança nacional, impedindo que esses ataques sejam frutíferos e sendo capazes de atacar de volta, em casos extremos, por saberem que em matéria de cibersegurnça, os adversários são manifestamente mais fracos.[111]

6.3. O consumismo no ramo tecnológico

Sendo os EUA uma superpotência mundial ao nível económico, têm uma procura muito elevada e por isso, uma produção igualmente extraordinária.

Tal como em todos os setores do mercado, o ramo tecnológico beneficia em grande parte da lei da oferta e da procura dos EUA, sendo aqui o berço de algumas das

---

[108] Ibidem.
[109] Ibid..., p. 16.
[110] The Washington Post, *The Cybersecurity 202: The United States is still number one in cyber capabilities*, https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/.
[111] Ibidem.

maiores empresas mundiais, tais como a Apple, Google e a Microsoft. O resultado é um alto grau de dependência global de produtos comerciais e de propriedade intelectual advinda dos EUA, tais como a tecnologia envolvida em microchips de computador, cabos de comunicação submarinos, satélites de comunicação e computação em nuvem, etc.[112] Além disso, existe também uma grande fonte de investimentos no ramo da alta tecnologia dos EUA, fazendo com que o capital total de investimento em empresas de tecnologia seja três vezes superior ao que podemos verificar na China.[113]

Mas tal como em tudo, existe sempre o outro lado da moeda, que neste caso é o facto dos EUA estarem muito mais dependentes do mundo tecnológico e do ciberespaço, do que qualquer outro país que se encontra abaixo dele, tendo uma maior responsabilidade no que toca à segurança aplicada a esse domínio. É por isso que, e tal como o título do presente subcapítulo indica, os EUA são um superpoder cibernético.

A economia digital nos EUA é a maior do mundo. De acordo com os estudos de 2018 da economia do país, 60% do crescimento nesse ano adveio da economia digital. [114] No entanto, apesar de todo o seu poder económico no ramo da tecnologia, os EUA contam com um mercado e uma cadeia de suprimentos globalizados, o que se tornou um grande problema aquando do governo de Donald Trump, uma vez que as suas políticas de proibição de utilização de chips manufaturados na China foram postas em ação numa altura critica da economia digital, levando a inúmeras queixas por parte do setor privado, já que muitas empresas de tecnologia e telecomunicação, incluindo gigantes como a Intel e a Motorola confiam na fabricação de peças na China para sustentar o seu modelo de negócio.[115]

Ao contrário daquilo que seria normal pensar, um ataque cibernético poderá ser muito mais prejudicial económica e financeiramente que, por exemplo, um furacão ou tornado. De acordo com um estudo feito pela Fundação para a Defesa de Democracias em conjunto com a empresa de seguros Intangic, a razão principal para isso são os efeitos indiretos que um ataque cibernético é capaz de causar, como por exemplo os danos

[112] IISS, *Cyber Capabilities and National Power: A Net Assessment, Research Papers*, 28 de junho de 2021, https://www.iiss.org/-/media/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---united-states.pdf, p. 18.
[113] Ibid..., p.19.
[114] Ibid..., p. 19.
[115] Ibid..., p.20.

causados à reputação de uma das empresas das quais a economia americana depende, impedindo que haja investimentos na mesma, causando custas inimagináveis a longo prazo.[116]

Ainda de acordo com o mesmo estudo, um hacker poderá causar prejuízos de 80 mil milhões de dólares com apenas um ciberataque suficientemente grande, enquanto que uma tempestade causaria, tomando por exemplo o furacão Sandy, cerca de 65 mil milhões de dólares em prejuízos.[117]

[116] The Washington Post, *The Cybersecurity 202: The United States is still number one in cyber capabilities*, https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/.
[117] Ibidem.

7. Os EUA, Rússia e China: o conflito

7.1. O início de uma corrida tecnológica.

O conflito tecnológico entre a Rússia e os EUA vem desde o final da Segunda Guerra Mundial, sendo necessário, por isso, regressar atrás no tempo para perceber quando começou e porque razão começou.

Depois do final da Segunda Guerra Mundial, um novo conflito começava. Conhecida como Guerra Fria, colocava as duas grandes potências mundiais – EUA democráticos e capitalistas e a URSS comunista – uma contra a outra. A partir do final da década de 1950, o espaço tornar-se-ia outra arena para a competição entre as duas superpotências, uma vez que cada lado queria provar a sua superioridade tecnológica, poder militar e, por extensão, o seu poder político-económico.[118]

A 4 de outubro de 1957, um míssil intercontinental soviético, lançava o *Sputnik*, o primeiro satélite artificial do mundo e o primeiro objeto feito pelo homem colocado no espaço. É claro que este lançamento foi uma surpresa total para os americanos, e uma surpresa bastante desagradável, uma vez que para os EUA, o espaço era ainda uma área desconhecida, mas de elevado interesse e que não podia ficar atrás da URSS.[119]

É então que em 1958, os EUA lançam o seu próprio satélite, chamado *Explorer I*[120], desenhado pelo exército dos EUA, sendo criada no mesmo ano a Administração Nacional de Aeronáutica e Espaço, comumente conhecida como NASA, dedicada somente à exploração do espaço.[121] Juntamente com a NASA, foram também criados dois programas com foco na segurança espacial, que iriam trabalhar em conjunto com a NASA. O primeiro posto em ação pela própria força aérea dos EUA, dedicando-se à potencial exploração militar do espaço, e o segundo posto em ação pela CIA, pela força aérea e por uma nova organização chamada *National Reconnaissance Office*.[122] Ambos

---

[118] History, *The Space Race*, https://www.history.com/topics/cold-war/space-race.
[119] Ibidem.
[120] NASA, *Explorer and Early Satellites*, https://www.nasa.gov/mission_pages/explorer/explorer-overview.html, [...].
[121] NASA, *NASA History*, https://www.nasa.gov/topics/history/index.html.
[122] History, *The Space Race,* https://www.history.com/topics/cold-war/space-race.

os programas teriam como objetivo final utilizar satélites em órbita para arrecadar informação sobre a URSS e os seus aliados.[123]

Em 1959, dá-se outro grande avanço no programa espacial soviético, com o lancaçamento do *LUNA 2*, a primeira sonda espacial a chegar à lua. É então que em 1961, Yuri Gagarin se torna a primeira pessoa a sair da órbita terrestre, viajando na cápsula espacial *Vostok 1*.[124] Até aqui, os EUA nunca tinham levado qualquer humano ao espaço, mas apenas chimpanzés em 1961. No entanto, teria ficado prometido pelo então Presidente John F. Kennedy que os EUA iriam aterrar na lua, antes do final da década.[125]

A promessa de Kennedy veio a ser cumprida no dia 20 de julho de 1969, aquando da aterragem de Armstrong e a sua famosa frase ‘’one small step for man, one giant leap for mankind’’.[126]

Ganhavam, então, os EUA a corrida espacial e tecnológica.

7.2. Rússia ou China? Qual o inimigo mais perigoso?

Como já foi mencionado anteriormente ao longo desta dissertação, a Rússia não é propriamente dotada da melhor cibersegurança comparativamente aos EUA, por exemplo. Ainda assim, os especialistas tendem a acreditar que a Rússia é bastante mais perigosa a curto prazo do que a China, uma vez que da segunda espera-se que seja um perigo a longo prazo.[127]

É claro que depende da definição de perigo que se atribui nesta situação específica, mas aqui a preocupação maior relativamente à Rússia é que se mostre como um maior perigo de causar dano a pessoas e organizações nos EUA, já que é nisso que os seus esforços tecnológicos recentes se têm fixado.[128]

---

123 History, *The Space Race*, https://www.history.com/topics/cold-war/space-race.
124 Ibidem.
125 Ibidem.
126 Ibidem.
127 The Washington Post, *Is Russia or China The Biggest Threat? Experts are split,* https://www.washingtonpost.com/politics/2022/01/20/is-russia-or-china-biggest-cyber-threat-experts-are-split/.
128 Ibidem.

Por outras palavras, podemos dizer que a Rússia poderá vir a causar danos rápidos e imprevisíveis enquanto que a China é uma ameaça estratégica com um processo mais demorado.

Além disso, e como temos vindo a observar com as últimas noticias no plano internacional, a Rússia tende a ter menos ‘’receio’’ de pressionar as feridas, e ir contra grandes organizações como a NATO, para levar a cabo os seus objetivos, descurando quaisquer tratados internacionais e soberania dos estados, tal como aconteceu com a invasão na Ucrânia.

A Rússia utiliza a tecnologia contra países que considera parte da sua influencia, ou seja, países que eram parte integrante da URSS, complementando a diplomacia energética, atividades de serviços secretos, apoiando governos instáveis com dinheiro e proteção, tudo para que possa manter a influencia russa nesses países.[129] Ao mesmo tempo, as capacidades de exploração de contra-rede russas são direcionadas aos sistemas de informação de empresas estatais, militares e de alta tecnologia ocidentais como parte dos esforços da espionagem russa.[130]

Os grupos de hackers russos, chamados de ‘’chapéu preto’’ por serem maioritariamente anónimos, são considerados líderes mundiais em cracking de software de computadores, e na criação e utilização de rookits.[131] Estes grupos operam, em regra, com aprovação tácita do governo russo, e obtêm rendimentos através das várias atividades traduzidas em crimes cibernéticos direcionadas ao ciberespaço ocidental.[132] Em troca, estes grupos criminoso têm a sua liberdade condicionada, desde que direcionem os seus recursos tecnológicos para alvos considerados adequados pelo governo.[133]

A Russian Business Network é o grupo mais conhecido, cujos botnets[134] atacaram através a Estónia através de uma tecnologia chamada DDOS, cujo objetivo é deixar um servidor, serviço ou infraestrutura indisponível ou fora de serviço.[135]

---

[129] Viktor Nagy, *The geostrategic struggle in cyberspace between the United States, China, and Russia*, National University of Public Service, Budapeste, 2012, p. 23.
[130] Ibidem.
[131] Pacote de software maligno projetado para oferecer acesso não autorizado a um computador ou outro tipo de software.
[132] Viktor Nagy, *The geostrategic struggle in cyberspace between the United States, China, and Russia*, National University of Public Service, Budapeste, 2012, p. 23.
[133] Ibidem.
[134] Grupo de computadores conectados através de um malware e controlados pelo próprio criados desse botnet.
[135] Viktor Nagy, *The geostrategic struggle in cyberspace between the United States, China, and Russia*, National University of Public Service, Budapeste, 2012, p. 23.

Ao contrário da China, a Rússia utiliza o ciberespaço para realizar campanhas de desinformação em larga escala no exterior, principalmente antes de eleições em países como os EUA.[136] Ainda que a Rússia seja líder em certos recursos cibernéticos e que possua algumas empresas bem estabelecidas no que toca às áreas relacionadas com software, não tem a indústria comercial que os EUA têm, para que seja possível apoiar o desenvolvimento tecnológico.[137] É por isso que a Rússia, ao contrário dos EUA irá sempre apostar em táticas de custo relativamente baixo, tais como ciberataques e campanhas de desinformação, continuando a ser uma característica fundamental da politica cibernética do Kremlin.

Quanto à China, a sua estratégia geral no que toca ao ciberespaço consiste em várias camadas.

Em primeiro lugar há que ter noção que, tal como a Rússia, a China é um país com visões muito diferentes daquelas que são as ocidentais e, por isso, essa visão molda o quão agressiva será na promoção do seu ponto de vista através dos meios digitais. Assim como Pequim vê o dólar como moeda internacional e base de todo o mercado internacional, também considera a aplicação da lei dos EUA a outros países e a interpretação ocidental da lei sobre a liberdade na internet como um caminho para Washington afirmar a sua influência no mundo.[138]

O tamanho do mercado da China é de extrema importância nesta análise, uma vez que lhe permite ditar os termos de negociação dentro do seu próprio país, tonando a discussão sobre os padrões do ciberespaço uma das primeiras em que Pequim tem um assento à mesa para argumentar legitimamente que é um concorrente dos EUA, e assim, uma voz com importância nesse debate.[139]

---

[136] Matthew Bey, *Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition*, 19 de setembro de 2022, https://www.jstor.org/stable/pdf/26554994.pdf?refreqid=excelsior%3A1f5b47051680b7cc1e3f81001ca31d2b&ab_segments=&origin=&acceptTC=1, p. 34.

[137] Ibidem.

[138] Matthew Bey, *Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition*, 19 de setembro de 2022, https://www.jstor.org/stable/pdf/26554994.pdf?refreqid=excelsior%3A1f5b47051680b7cc1e3f81001ca31d2b&ab_segments=&origin=&acceptTC=1, p. 32.

[139] Ibidem.

A inteligência tecnológica da China é coordenada e dirigida por várias agências governamentais, mas é baseada em botnets operados por criminosos organizados e no grande número de hackers patrióticos integrados em vários grupos, sendo o maior deles a Red Hacker Alliance, sempre disposta a trabalhar para o governo chinês.[140] O software malicioso chinês tem a capacidade de colocar em perigo praticamente qualquer computador conectado à internet, o que significa que os computadores que executem diretamente o software chinês, podem estar fisicamente localizados em qualquer país, o que dificulta a tarefa de rastrear a origem de um ataque cibernético.[141]

Na maioria das vezes, os computadores e outros produtos de tecnologia são frequentemente infetados com malware antes de saírem da fábrica, sendo os seus principais alvos os governos estrangeiros, forças armadas, defesa nacional e outras empresas de alta tecnologia. [142]

Tal como supramencionado, a lei da oferta e da procura tem um grande impacto no avanço tecnológico de cada país. Enquanto que a China oferece mão de obra muito barata e tecnologia relativamente avançada, a verdade é que os salários da maioria dos cidadãos chineses são extremamente baixos, e o custo de vida, em comparação com o salário mínimo, é muito alto, levando a que o cidadão ‘’comum’’ não consiga ter acesso a bens que para o americano é normal conseguir. Qualquer cidadão americano tem um iPhone, um portátil de última geração, o melhor televisor com a tecnologia mais avançada, isto porque o salário mínimo em comparação com o custo de vida é realmente melhor que noutros países considerados rivais no mundo digital.

Podemos concluir, ainda assim, que os EUA continuam no pódio, em primeiro lugar na corrida cibernética, mas a realidade é que a posição poderá vir a mudar ao passo que mudam outros fatores internacionais, tais como flutuações de mercados, mudança de governos, etc.

O mundo digital é demasiado inconstante para que se possa considerar que um país tem o monopólio tecnológico assegurado. Todos os dias saem novas tecnologias de ponta, novos produtos virais, e as redes sociais também são a prova disso. O Facebook,

---

[140] Viktor Nagy, *The geostrategic struggle in cyberspace between the United States, China, and Russia*, National University of Public Service, Budapeste, 2012, p. 21.
[141] Ibidem.
[142] Ibidem.

originalmente idealizada nos EUA, começou por ser a rede social mais utilizada de sempre, para passar a ser uma das menos utilizadas. Como exemplo da flutuação de mercados e incapacidade de monopolizar o mundo digital, temos o *Tiktok*, uma rede de origem chinesa, que por sua vez é a rede com mais usuários neste momento.

8. O uso da internet como arma de guerra

8.1. As redes sociais

A rápida expansão da Tecnologia da Informação criou um ambiente onde as informações estão prontamente disponíveis e qualquer pessoa interessada pode aceder a qualquer site, onde encontrará aquilo que procura. Hoje em dia, qualquer pessoa com um smartphone ou um computador, com a ajuda da internet, pode adquirir, processar e transmitir uma grande quantidade de informações capazes de chegar a todo o mundo. A internet desempenha agora um papel cada vez mais importante em todos os tipos de atividades diárias, desde a organização mundial mais importante, até ao comum cidadão que a utiliza diariamente.

As redes sociais têm sido justamente celebradas como uma ferramenta habilitante para os cidadãos comuns se mobilizarem contra as mais variadas injustiças, tais como governos repressivos, situações de injustiça social e também permitindo que se façam ouvir as suas vozes marginalizadas. Mas a questão crucial permanece sem resposta: porque é que os Estados sedentos de poder, com controle sobre o acesso à internet devem ceder impassivelmente à derrota? A resposta simples é: não cedem.

Desde muito cedo que com o avanço da rede online os governos começaram a aperceber-se que seria fácil controlar todos os passos dos seus cidadãos, e de cidadãos de outros países através da internet. A realidade é que todos nós fazemos a nossa vida online. Desde transferências bancárias, a consultar documentos, a trabalhar, a interagir com os nossos amigos e família, tudo é feito através da internet, sem termos noção que podemos estar constantemente a ser vigiados.

A guerra civil na Síria, que custou centenas de milhares de vidas é um exemplo disso. De acordo com especialistas, a pressão do governo de Obama para desencadear uma ação militar contra a Síria em agosto de 2013, começou com vídeos e imagens que circularam online, descrevendo as terríveis consequências de um suposto produto químico que teria sido usado no ataque a East Ghouta.[143] Nestes vídeos era possível ver

[143] Marc Lynch, Deen Freelon, Sean Aday, *Syria's Socially Mediated Civil War,* United States Institute of Peace, 2012, https://www.usip.org/sites/default/files/PW91-Syrias%20Socially%20Mediated%20Civil%20War.pdf, p. 5.

filas de crianças mortas, alinhadas no chão de pedra, algo que foi capaz de moldar decisivamente o decurso da guerra.[144] O regime da Síria expandiu ativamente a sua presença virtual desde a contratação de um ‘’exército de hackers’’ até ao uso de uma série de softwares de espionagem contra toda a sua população.[145] Para intercetar as informações e comunicações dos utilizadores sírios do *Facebook*, o regime lançou ataques que permitiam terceiros acederem e modificarem o conteúdo do utilizador, chegando a torturar pessoas para que lhes dessem a sua senha e nome de utilizador do Facebook.[146]

De acordo com uma entrevista feita pela Universidade da Pensilvânia, a Peter Singer e Emerson Brooking, autores do livro *LikeWar*, a ISIS e outras organizações terroristas, têm entrado em contacto com pessoas nas redes sociais para as recrutarem para os seus movimentos.[147] Em 2014, aquando da invasão do norte do Iraque, a ISIS tinha apenas 1500 militantes, mas tudo isso mudou quando puseram em prática uma nova estratégia através da qual publicavam no *Twitter* com a *hashtag #AllEyesOnISIS*, na qual consolidavam e transmitiam a sua propaganda.[148] A verdade é que embora a tática pareça pouco provável de funcionar, foi capaz de causar o pânico geral e até levou cidades como Mosul a baixar as armas e fugir a uma guerra com a ISIS, sendo também capaz de recrutar mais de 30.000,00[149] combatentes do Médio Oriente e do resto do mundo.

O problema que se coloca com o uso das redes sociais e da internet como arma de guerra, é que é um sitio onde uma panóplia de sujeitos atua com diferentes objetivos, e acabam utilizando táticas muito semelhantes por serem capazes de observar a sua eficácia noutros ataques e ações outrora postos em prática.[150] Neste momento existem milhares de organizações e sujeitos com más intenções a entrar em contacto com pessoas comuns para as aliciar a alinhar nas suas ideias. Quem é que nunca recebeu, por exemplo, uma

---

144 Ibidem.
145 The Hacker News, *The Syrian spyware to targe the opposition activists*, https://thehackernews.com/2012/02/syrian-spyware-to-target-opposition.html.
146 Harvard Kennedy School, Shorenstein Center on Media, Politics and Public Policy, *Social Media used by regime and activists in Syrian Revolution, says NPR's Deborah Amos*, https://shorensteincenter.org/speaker-series-with-nprs-deborah-amos/.
147 Knowledge at Wharton, *Why Social Media Is the New Weapon in Modern Warfare*, https://knowledge.wharton.upenn.edu/article/singer-weaponization-social-media/.
148 Ibidem.
149 Ibidem.
150 Ibidem.

mensagem para se juntar a um esquema em pirâmide? Quem é que nunca recebeu uma mensagem com um link estranho que ao tocar pedia que colocássemos as nossas credenciais?

Como foi explorado no capítulo I, até nas eleições são utilizadas as redes sociais para levar a cabo as ideologias de quem concorre, como no caso de Trump que contratou a *Cambridge Analytica*. É por isso que, no capítulo seguinte, iremos explorar o porquê da necessidade de cibersegurança, e de um regime jurídico internacional capaz de contrarreagir a esses ataques.

8.2. A primeira Guerra Cibernética

A maioria das grandes guerras do século XX tiveram o seu próprio meio digital de acompanhamento conforme a época em que ocorreram. O filme na Segunda Guerra Mundial, televisão no Vietname, transmissão ao vivo na Guerra do Golfo, entre outras. Mas a guerra pelo Kosovo é considerada o primeiro conflito armado em que todos as partes integrantes da guerra tinham presença ativa na internet. É por isso que é considerada a primeira Guerra Cibernética.[151]

Para melhor compreender este conflito, passemos a uma breve introdução:

Em 1989, Ibrahim Rugova, líder dos albaneses na província Sérvia do Kosovo, iniciou uma politica de protestos não violentos contra a abrogação da autonomia constitucional da província, levada a cabo por Slobodan Milosevic, então presidente da república da Sérvia.[152] Em 1991, as coisas começam a mudar, e após uma votação secreta, os albaneses étnicos proclamam a criação de uma república própria do Kosovo, embora sem grande reconhecimento internacional.[153] É então que em 1996 aparece o Kosovo Liberation Army, que vem por em ação ataques esporádicos contra autoridades Sérvias no Kosovo.[154]

---

[151] PK Mallick, *Internet – A Weapon of War*?, The Centre for Land Warfare Studies, https://www.researchgate.net/publication/344737617, março 1999, p. 6.
[152] Britannica, *Kosovo Conflict*, https://www.britannica.com/event/Kosovo-conflict.
[153] Frontline, *A Kosovo Chronology*, https://www.pbs.org/wgbh/pages/frontline/shows/kosovo/etc/cron.html.
[154] Ibidem.

A partir de 1998, a tensão entre os separatistas aumentava, dando-se cada vez mais ataques contra as autoridades sérvias, e levando a que os albaneses controlassem certas partes da província. Após uma tentativa falhada de negociar a paz sobre o conflito separatista, a NATO atacou a Jugoslávia no final de março de 1999, dando início à Guerra do Kosovo. A 3 de junho do mesmo ano, dava-se o fim da guerra com a retirada das tropas sérvias, permitindo a paz internacional no Kosovo, sendo nomeado um governo provisório, sob tutela da ONU.[155]

A guerra no Kosovo era muito diferente das demais anteriores, não pelo seu objetivo principal, mas pela forma como era partilhada no mundo: através da internet. Qualquer pessoa que quisesse saber mais sobre o conflito, podia simplesmente procurar a informação que estava disponível, pela primeira vez, online, desde atualizações diárias de direitos humanos da Macedónia, até proclamações jugoslavas.[156]

Atores governamentais e não governamentais usavam a internet para disseminar informação, propaganda, descredibilizar oponentes e pedir ajuda e apoio para a sua posição. Por outro lado, os hackers usavam a internet para expor as suas objeções contra a agressão por parte da Jugoslávia e da NATO, através do ataque a computadores e entrando nos websites para os desconectar da rede. Do outro lado, tínhamos os cidadãos comuns que viam na internet uma forma de contar as suas experiências de horror e medo diários, dentro da zona de conflito, enquanto os ativistas se aproveitavam delas para sensibilizar o mundo para aquilo que estava a acontecer.[157]

A internet oferecia acesso a um ponto de acesso sem censura por parte da Sérvia, havendo possibilidade do caso sérvio estar muito mais bem representado online e próximo daquela que era a realidade, já que não haviam filtros. Todos os dias a NATO publicava imagens de um satélite espião que mostrava o que tinham sido capazes de atingir e a situação humanitária no Kosovo.[158] Ambos os lados da guerra estavam presos numa feroz

---

155 Ibidem.

156 PK Mallick, *Internet – A Weapon of War*?, The Centre for Land Warfare Studies, https://www.researchgate.net/publication/344737617, março 1999, p. 9.

157 John Arquilla, David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defense Research Institute, RAND, California, 2001, pp. 239 a 240.

158 PK Mallick, *Internet – A Weapon of War*?, The Centre for Land Warfare Studies, https://www.researchgate.net/publication/344737617, março 1999, p. 6.

cruzada de informações. Na TV, no rádio e na internet, a batalha da informação continuava.[159]

Ambos os lados afirmavam que o outro estava a distorcer a verdade com mentiras e propaganda. Mas a NATO foi mais longe ao tratar a rádio e a televisão jugoslavos como um alvo militar para incitar uma limpeza étnica, chegando a declarar que a Rádio e a TV sérvias tinham ‘’sangue nas mãos’’.[160] Como resposta, a Jugoslávia procedeu a ataques cibernéticos às redes e computadores da NATO, mas sempre sem sucesso.

A internet teve um grande impacto nas decisões tomadas quanto a políticas estrangeiras relativamente à guerra. Enquanto a NATO atacava os media tradicionais que espalhavam a propaganda de Milosevic, escolhia não bombardear o serviço de internet na Jugoslávia, ou sequer deitar abaixo os servidores. A ideia era deixar a internet sempre funcional, já que a mesma era a única forma de comunicação livre de censura por parte da Sérvia, e permitiria que o povo servo conseguisse ter a verdadeira noção das atrocidades que estavam a ser cometidas contra o Kosovo.[161]

Podemos, por isso, concluir que a internet além de ser uma poderosa ferramenta de partilha de informação, pode também ser uma arma de guerra, capaz de mudar o seu decurso e determinar o desencadeamento final.

[159] Ibidem.
[160] Ibidem.
[161] John Arquilla, David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, National Defense Research Institute, RAND, California, 2001, pp. 241 a 243.

CAPÍTULO III

9. Cibersegurança: uma necessidade premente

9.1. O que é a cibersegurança? E como funciona?

A cibersegurança é a prática de proteger sistemas, redes online e programas de ataques digitais.[162] O seu objetivo principal é reduzir o risco de ataques cibernéticos e a proteção contra a exploração não autorizada de sistemas, redes online e tecnologias.[163]

No entanto, para melhor perceber o conceito, há que estudar doutrina acerca da matéria.

De acordo com Mulligan e Schneider, existe um pré-requisito para poder definir o termo cibersegurança e colocá-lo em prática contra os ciberataques: é preciso especificar os objetivos e meios.[164] De acordo com os mesmos:

- Os objetivos definem que propriedades de sistema irão ser preservadas, tais como quais as políticas a serem reforçadas, para quem, a que preço, e contra quais ameaças. Os objetivos podem ser absolutos, ou especificar uma série de permissões para negociar. Ao permitir as negociações, reconhecemos a natureza política da cibersegurança e a necessidade premente da mesma;
- Os meios envolvem medidas tecnológicas, educacionais e/ou regulamentares. É expectável que esses meios incluam políticas que criam incentivos, que podem variar entre meios de coação ou meios com base nas flutuações do mercado, capazes de incitar à adoção das medidas propostas.[165]

Mulligan e Schneider defendem que a cibersegurança é um bem público e deve ser acessível a todos, tal como acontece com a saúde, por exemplo.

Desde muito cedo que os engenheiros informáticos se depararam com um problema nascido da tecnologia que eles próprios haviam criado. Se era tudo compartilhado através de um sistema, como é que podiam proteger esse sistema? A

---

[162] CISCO, *What is Cybersecurity*?, https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

[163] ITGovernance, *What is Cybersecurity? Definition and Best Practices*, https://www.itgovernance.co.uk/what-is-cybersecurity.

[164] Deirdre K. Mulligan, Fred B. Schneider, *Doctrine for Cybersecurity,* 2011, p.71.

[165] Ibidem.

verdade é que inicialmente toda a doutrina que existia sobre tecnologia era voltada apenas para a inovação e nunca para a proteção, uma vez que havia um número muito reduzido de pessoas a utilizar as redes dos sistemas de computação.[166]

O problema é que as soluções para criar a isolação necessária para proteção dos sistemas estavam muito aquém das capacidades dos engenheiros já que não era essa a principal preocupação dos mesmos e, por isso, nunca tinham sido exploradas e estudadas. O avanço tecnológico não é o único meio através do qual se resolvem problemas criados pela tecnologia.

Os ciberataques são um perigo iminente para organizações, trabalhadores e consumidores. Estes ataques podem ser engenhados para aceder ou destruir informação sensível ou até mesmo para extorquir dinheiro. Podem, de facto, destruir negócios, economias, e até o nosso próprio estado financeiro e vida pessoal.

De acordo com o relatório de 2021 do ITRC acerca de violação de dados, houve um aumento de 68% nos acessos não autorizados a dados pessoais presentes em redes digitais nos EUA entre 2020 e 2021.[167]

A cibersegurança vem ser criada exatamente para proteger os nossos dispositivos contra esse tipo de ataques.

À primeira vista parece ser um conceito bastante complicado, e é, mas para o cidadão comum, que nunca trabalhou com engenharia de computadores, é possível entender do que se trata através de um simples programa: um antivírus. Todo o utilizador de computadores, tablets ou telemóveis já deu de caras com a possibilidade de instalar um antivírus para proteger a informação que armazena nesses dispositivos.

O *software* antivírus procura, deteta e remove vírus e outros *softwares* maliciosos, como *worms*, *trojans*, *adware* e muito mais do dispositivo onde é instalado. Este tipo de programa é utilizado como prevenção à segurança cibernética, ou cibersegurança, e é capaz de interromper ameaças antes delas entrarem nos nossos dispositivos para causar problemas.[168]

---

[166] Ibidem.

[167] Norton, *What is cybersecurity? What you need to know*, https://us.norton.com/blog/malware/what-is-cybersecurity-what-you-need-to-know#.

[168] SOS Can Help, *How does Antivirus work*, https://www.soscanhelp.com/blog/how-does-antivirus-work#what.

É claro que, os programas antivírus que instalamos nos nossos computadores são muito menos complexos que aqueles utilizados por grandes organizações tais como a ONU, ou até mesmo aqueles utilizados por governos, que protegem grandes compêndios de informação secreta como, por exemplo, segredos de estado.

9.2. A cibersegurança nos EUA

Sendo os EUA a maior potência mundial a nível tecnológico, é de esperar que a sua proteção seja igualmente soberana. É, então, pertinente, estudar que tipo de cibersegurança é utilizada pelas agências governamentais do governo dos EUA, para que a informação possa ser protegida.

Em 2014, o governo norte-americano aprendeu o quão importante a segurança cibernética é, quando em março o Office of Personnel Management, que contem as informações pessoais de todos os funcionários federais e de qualquer pessoa que se tenha candidatado a um emprego no governo, foi hackeado.[169] Mais de 20 milhões de pessoas tiveram as suas informações comprometidas, tendo o governo pago pelo monitoramento de crédito gratuito de cada uma das vítimas, por forma a ajudar a remediar a situação.[170]

Para evitar este tipo de ataques, as agências governamentais tiveram de investir consistentemente em desafios de segurança cibernética. Alguns deles são:

- A Inteligência Artificial (IA) e Aprendizagem de Máquina (AM) – em que as ferramentas cibernéticas mais recentes utilizam a análise de comportamentos para impedir os sujeitos de má índole e impedir que a propriedade intelectual e os dados confidenciais caiam nas mãos erradas. Essas análises de ponta a ponta funcionam em ambientes de dados para identificar e interromper ameaças ao tráfego de rede, arquivos e dispositivos, aproveitando análises de comportamento do utilizador que se tornam mais inteligentes com o decurso do tempo. IA e AM podem agora fornecer visibilidade completa do utilizador para a deteção proactiva de ameaças, avaliação de ameaças em tempo real e gestão de riscos;[171]

[169] NITAAC, *The Importance of Technologies in Government*, https://nitaac.nih.gov/resources/articles/importance-cyber-technologies-government.
[170] Ibidem.
[171] bidem.

- Sistemas de deteção e prevenção de intrusão – conhecidas como ferramentas IDS e IPS, ajudam a equipa de engenharia eletrónica a identificar e proteger as suas redes com, e sem fios, contra vários tipos de ameaças à segurança. Essas tecnologias, tal como outras ferramentas de segurança de rede, tornaram-se mais populares à medida que as redes governamentais aumentaram a sua complexidade. As soluções IDS e IPS são capazes de detetar atividades ameaçantes na forma *malware, spyware,* vírus e *worms*, e outros tipos de ataque, bem como ameaças representadas por violações de políticas digitais. As ferramentas IDS monitorizam e detetam atividades suspeitas, já as IPS realizam a monitorização ativa e em linha e podem impedir ataques de fontes conhecidas e desconhecidas. Ambos os tipos de ferramentas podem identificar e classificar os tipos de ataque melhorando a segurança geral do dispositivo;[172]
- *Antimalware* – as ferramentas *antimalware* ajudam os administradores a identificar, bloquear e remover *malwares*. O principal objetivo dos *malwares* é procurar vulnerabilidades na rede, especialmente em defesas de segurança, sistemas operacionais, navegadores, aplicativos e alvos populares, como o *Adobe Flash, Acrobat* e *Reader*. As práticas recomendadas exigem uma defesa multifacetada que também pode incluir uma lista negra de IP, ferramentas de prevenção de perda de dados, *software* antivírus e *antispyware*, politicas de navegação na internet, filtragem de saída e *proxys* de tráfego de saída;[173]
- Gestão de dipositivos móveis – também chamado de MDM, esta solução permite aos administradores monotorizar e controlar remotamente as configurações de segurança em dispositivos móveis. Isto permite que os funcionários trabalhem à distância em dispositivos aprovados pela agência, mas sabendo que esses dispositivos são seguros porque podem geri-los a todo o tempo;[174]
- Controlo de acesso à rede – esta tática reforça a politica de segurança, concedendo acesso aos ativos da rede apenas aos dipositivos que se encontrem em conformidade com a política de acesso. Lidam com funções de autenticação e autorização e podem controlar os dados a que utilizadores específicos acedem,

[172] bidem.
[173] Ibidem.
[174] Ibidem.

garantindo que os utilizadores passem por um determinado padrão de segurança antes de poderem aceder a qualquer informação;[175]

- *Firewalls* de última geração – a tecnologia além daqueles que eram os *firewalls* tradicionais foi expandida. Os *firewalls* de ultima geração fornecem serviços de segurança de rede aprimorados, incluindo visibilidade e controlo de aplicações, juntamente com os fundamentos de segurança na internet;[176]
- Autenticação e autorização – os serviços tradicionais baseados em autenticação de utilizadores concedem acesso a determinada informação com base nas regras de autorização projetadas por aquele serviço especifico. A tecnologia de segurança baseada em identidade mais recente usa métodos como certificados digitais e soluções de infraestrutura de chaves públicas que fornecem uma camada extra de segurança.[177]

É desta forma que os EUA se mantêm como o país em primeiro lugar na corrida tecnológica, não tanto a nível de capacidade de ataque, mas mais a nível de segurança cibernética contra esses ataques.

[175] Ibidem.
[176] Ibidem.
[177] Ibidem.

10. O Impacto da Tecnologia nas Políticas da Organização das Nações Unidas

10.1. The High Level Panel on Digital Cooperation

A 12 de Julho de 2018, o Secretário Geral das Nações Unidas, António Guterres, estabeleceu o *High-Level Panel on Digital Cooperation,* com o objetivo de fortalecer a cooperação global a nível digital para garantir um futuro digital seguro e inclusivo para todos[178]. De acordo com o *website* oficial das Nações Unidas, o propósito do painel é conseguir acompanhar a escala, a difusão e velocidade das mudanças trazidas pela tecnologia digital já que as mesmas não têm precedentes, levando a que os meios atuais e níveis de cooperação sejam desiguais para o desafio que enfrentamos.[179]

O painel é composto por 20 membros independentes de variados ramos incluindo membros de governos, indústria, sociedade civil e comunidade técnica.[180] Reuniu pessoalmente duas vezes, uma em Setembro de 2018 e outra em Janeiro de 2019, e reúne quando necessário por meios remotos. No final de cada reunião o painel submete as deliberações e relatórios, incluindo recomendações acionáveis dentro de um período de 9 meses.[181]

Em Junho de 2020, o Secretário Geral apresentou um conjunto de ações para a comunidade internacional certificar que todos estão conectados, respeitados e protegidos na era digital:

- ‘’Achieving universal connectivity by 2030 – everyone should have safe and affordable access to the internet;
- Promoting digital public goods to unlock a more equitable world – the internet’s open source, public origins should be embraced and supported;
- Ensuring digital inclusion for all, including the most vulnerable – under-served groups need equal access to digital tools to accelerate development;
- Strengthening digital capacity building – skills development and training are needed around the world;

[178] Edson Prestes, *An Overview of the United Nations High-Level Panel on Digital Cooperation,* https://www.researchgate.net/publication/331664721_An_Overview_of_the_United_Nations_High-Level_Panel_on_Digital_Cooperation_Industry_Activities, 12 de março de 2019, p. 103.
[179] United Nations, *Civil Society*, https://www.un.org/en/civil-society/secretary-general’s-high-level-panel-digital-cooperation.
[180] Ibidem.
[181] Ibidem.

- Ensuring the protection of human rights in the digital era – human rights apply both online and offline;
- Supporting global cooperation on artificial intelligence that is trustworthy, human-rights based, safe and sustainable and promotes peace;
- Promoting digital trust and security – calling for a global dialogue to advance the Sustainable Development Goals;
- Building a more effective architecture for digital cooperation – make digital governance a priority and focus the United Nations' approach''.[182]

No que toca ao ramo dos direitos humanos e segurança, o painel recomendou que as Nações Unidas revissem como é que os acordos internacionais sobre os direitos humanos se aplicam relativamente às novas tecnologias, além de ter recomendado que as empresas de redes sociais trabalhassem em conjunto com os governos, internacionalmente e localmente para que houvesse uma resposta mais célere aquando da violação de direitos humanos.[183] Além disso, recomendou, também, que António Guterres facilitasse a abertura de um processo de consulta para desenvolver mecanismos atualizados de combate à falta de acesso ao mundo digital por parte das populações.[184]

As mais recentes atividades do painel passaram pelo lançamento da campanha ''Call for Contributions'', na qual mais de 100 contribuições foram recebidas por *stakeholders* de uma vasta gama de partes interessadas que refletiram sobre os valores e princípios orientadores da cooperação digital.[185] Além disso, organizou um diálogo regional com a região africana em colaboração com a Comissão da União Africana, a Comissão Económica das Nações Unidas para África, a União Internacional de Telecomunicações (UIT), o Fórum de Governança da Internet (IGF), a Corporação da Internet para Nomes e Números Atribuídos (ICANN), a Association for Progressive Communication (APC) e a DiploFoundation, para reunir ideias sobre as recomendações feitas pelas mesmas, e promover a cooperação e inovação digital regional.[186]

10.2. E-democracy and Diplomacy: as Nações Unidas na Era Digital

[182] Ibidem.
[183] SDG Knowlege Hub, *UN High-Level on Digital Cooperation Calls for 2020 Global Commitment,* *https://sdg.iisd.org/news/un-high-level-panel-on-digital-cooperation-calls-for-2020-global-commitment/*.
[184] Ibidem.
[185] Digwatch, *The UN High-Level Panel on Digital Cooperation,* https://www.dig.watch/processes/hlp.
[186] Ibidem.

As organizações internacionais, tais como as Nações Unidas ou a União Europeia, são criadas para fomentar a cooperação e harmonizar as relações e as ações dos Estados na prossecução de objetivos comuns. É claro que, com a globalização, o processo de comunicação entre sujeitos internacionais tem passado por significativas mudanças, levantando problemas que outrora não se verificavam.

Desde a invenção do telégrafo, do telefone e dos computadores, deixou de ser necessário esperar meses por uma carta para que se pudesse comunicar de um país para o outro, mudando completamente a esfera das relações internacionais. Hoje em dia, com as redes sociais e plataformas online, ‘’mudam os prazos para as relações diplomáticas, oferecendo uma potencial transformação no que toca à definição da agenda e enquadramento de questões’’.[187]

A partir de meados dos anos 2000 e até aos dias que correm, temos visto uma aderência cada vez maior por parte da ONU às redes sociais, incluindo no *Facebook*, onde está ativa desde 2007, e no *Twitter* onde ativou a conta pela primeira vez em 2008.[188] A partir daí, foi criado um gabinete especifico para as redes sociais da ONU – *The Department of Global Communications* – que trata de todos os canais digitais da mesma, sejam eles no Instagram, Youtube, Pinterest ou qualquer outra plataforma *mainstream.*[189]

Como mencionado anteriormente, desde a eleição de António Guterres como Secretário Geral da ONU, diversas medidas têm sido postas em prática para acompanhar o crescimento e desenvolvimento do mundo digital, nomeadamente através do *High-Level Panel on Digital Cooperation.* No entanto, aquando da criação do painel, não foram dadas diretivas à restante organização, no que toca ao processo de adaptação às medidas implementadas. Em vez disso, esse assunto foi tratado aquando da publicitação da ‘’Estratégia do Secretário-Geral da ONU sobre Novas Tecnologias’’ em Setembro de 2018.[190] Embora esta estratégia não aborde especificamente a questão da integração de ferramentas digitais nos processos da ONU, indica claramente a vontade da organização em refletir sobre o uso e impacto das novas tecnologias no seu trabalho e ação internacional.

---

[187] Corneliu Bjola, Ruben Zaiotti, *Digital Diplomacy and International Organisations: Autonomy, Legitimacy and Contestation,* Routledge, New York, 2021, p. 103.
[188] Ibid…, p. 104.
[189] Ibidem.
[190] Ibid…, p. 105.

Se nos basearmos na doutrina sobre organizações internacionais, especificamente na ONU e na própria sociologia organizacional conseguimos identificar vários factores que entram em jogo nos processos da ONU. Mas os mais importantes são:

1. Regras de procedimento;
2. Interações estratégicas;
3. Rede informal.[191]

Estes três ramos foram os mais afetados pela era digital, de acordo com estudos recentes.

10.3. The UN Secretariat's Department Of Global Communications

Em 1946 foi criado o *Department of Public Information* (doravante DPI), como parte integrante do Secretariado da ONU, como promotor, na medida do possível, de uma compreensão informada do trabalho e dos propósitos das Nações Unidas entre a população mundial.[192] Este departamento continua ativo, embora as suas responsabilidades e competências tenham evoluído com o passar dos anos, tendo passado a ser responsável pela formulação e implementação das estratégias de comunicação interna e externa da organização, e tendo passado a chamar-se *Department of Global Communications* a partir de Janeiro de 2019.[193]

Uma das grandes mudanças a nível interno na ONU aquando da mudança digital, prende-se com a redefinição de *regras de processamento* na comunicação e partilha de informação no Secretariado da organização.[194] Como mencionado supra, desde meados dos anos 2000 a ONU tem vindo a desenvolver novas estratégias de comunicação. Em 2005 foi introduzido um novo programa chamado *'iSeek''* que permitia que houvesse uma rede interna dentro da própria organização, ligando esferas diferentes da mesma numa só plataforma.[195] Esta plataforma veio apresentar-se como extremamente útil em tempos de crise. Tomando como exemplo o tremor de terra no Haiti em 2010, foi

[191] Ibidem.
[192] Ibid…, p. 110.
[193] Ibidem.
[194] Ibid…, p. 111
[195] Ibidem.

importantíssimo manter informação atualizada sobre os acontecimentos em tempo real, bem como a manutenção da comunicação entre membros da organização, já que foram perdidos mais de 102 colaboradores.[196] No entanto, a plataforma mostra-se obsoleta nos dias de hoje e é por isso que em 2019 foi atualizada com uma nova plataforma chamada *''e-deleGATE''* que permite que a base de dados para comunicação facilitada não seja apenas interna, mas também externa, levando assim a que a organização possa estar em constante contacto com os Estados Membros.[197]

Quanto às *interações estratégicas*, o foco principal das mesmas foram as redes sociais. Inicialmente, as redes sociais eram vistas apenas como uma forma de chegar aos indivíduos, e não como uma ferramenta política. No entanto, hoje em dia as redes sociais são vistas pela ONU como uma enorme componente da estratégia de comunicação.[198] A escolha de que redes sociais usar e quando publicar nas mesmas tem por detrás a natureza do evento ou comunicação a ser feita.[199] Em 2017, o *Department of Global Communication* lançou uma campanha para encorajar todos os utilizadores destas plataformas a ser ativos na luta pela mudança ambiental. Esta campanha foi desenvolvida em conjunto com o *Facebook* e permitia que os utilizadores conseguissem comunicar com um robot dotado de inteligência artificial, capaz de responder a questões dos utilizadores sobre o ambiente e aquecimento global.[200] Esta campanha permitia que o utilizadores tivessem acesso rápido e gratuito a informação pertinente sobre um problema atual e que depende de toda a população para ser solucionado.

Finalmente, e no que toca às *redes informais,* estas foram, talvez, as que menos sofreram alterações com a era digital. De acordo com as Nações Unidas, a rede social mais utilizada para partilha de ações tomadas pela organização é o *Twitter.*[201] Além de possibilitar a publicitação em tempo real da ação da ONU, também cria uma relação mais próxima com os cidadãos. Dentro das redes informais existem dois tipos de entidades: os *adopters* e os *change agents*, havendo dos tipos de *adopters (innovators and early*

196 Ibidem.
197 Ibid…, p. 113.
198 Ibidem.
199 Ibid…, p. 113.
200 Ibid…, p. 115.
201 Ibidem.

adopters).[202] Os membros da *Social Media Team* são os *early adopters,* já os dos outros departamentos dentro da ONU são os *innovators.*[203]

As redes sociais e avanços tecnológicos tiveram um impacto muito positivo na política atual da ONU, no entanto, também acabaram por produzir vários efeitos imprevistos e indiretos. Um dos maiores problemas que se levantou foi o embaçar da linha que dividia a comunicação interna e a externa, e as potenciais repercussões que isso teve a nível da reputação da própria Organização.[204] Em 2011, o *Department of Public Information* argumentou que as ferramentas das redes sociais criaram desafios à medida que a distinção entre comunicação interna e externa, e profissional e comunicativa é muitas vezes confusa e precisa de ser regulamentada através de diretrizes e diretivas.[205] Essas diretivas passariam por alertar a equipa que deveriam ter cuidado na utilização das redes sociais, sendo dotados de discrição, já que as portagens poderiam ser interpretadas como declarações oficiais ou até compromissos feitos pela ONU, pedindo, ainda, que no que toca à comunicação interna da empresa, não fosse feita apenas através do canais digitais, dando prioridade às reuniões presenciais.[206]

10.4. Blockchain: O Impacto No Desenvolvimento Sustentável Das Nações Unidas

A tecnologia *Blockchain* é considerada uma nova classe, tal como outrora foi a internet, ou um novo tipo de tecnologia dentro da própria internet.[207] Para perceber de que forma funciona, é necessário começar pelas noções básicas de *Blockchain.*

Distributed Ledger Technology ou DLT é a base da *Blockchain,* porque oferece um mecanismo de validação consensual, através de uma rede de computadores, que facilitam as transações ponto a ponto, sem que haja necessidade de um intermediário ou

---

202 Ibid…, p. 116.
203 Ibidem.
204 Ibid…, p. 117.
205 Ibidem.
206 Ibid…, p. 119.
207 Marco André da Silva Costa, Abdelhamid Nedzhad, Danijela Lucic, *Designing a Digital Education Ecosystem,* https://www.researchgate.net/profile/Venelin-Terziev/publication/351956534_DESIGNING_A_DIGITAL_EDUCATION_ECOSYSTEM/links/60b21574a6fdcc1c66ec67a0/DESIGNING-A-DIGITAL-EDUCATION-ECOSYSTEM.pdf#page=152, 2021, p. 146.

de uma autoridade centralizada para atualizar e manter as informações geradas por essas transações.[208] Cada vez que uma transação é validada é adicionada a um novo ‘’bloco’’ de transações previamente validadas, dando origem ao nome *Blockchain.*[209] Assim que é adicionada a esse bloco já não pode ser alterada ou removida.[210] As organizações podem desenvolver a sua própria rede ou personalizar uma rede básica previamente desenvolvida por um vendedor.[211] A tecnologia *Blockchain* revolucionou a forma de armazenar, administrar e transferir documentos e valores entre identidades digitais e muito dos setores da economia, facilitando negócios baseados em transações.[212]

Recentemente, a *Blockchain* evoluiu para uma nova tecnologia chamada *Impact Tokens*, que por sua vez representam um link para um dos Objetivos de Desenvolvimento Sustentável das Nações Unidas, geralmente na forma de uma unidade ou medida quantificáveis, que estão ligadas à atividade que a criou.[213] Estes *tokens* podem ser utilizados para fazer pagamentos de acordo com o desempenho da organização, registar impactos ao longo da cadeia de abastecimento, ou ser a própria cadeia de abastecimento, e, ainda, destacar ações para apoiar os Objetivos de Desenvolvimento Sustentável.[214] A *Blockchain* é provavelmente a aplicação tecnológica mais utilizada no ramo do apoio comunitário, uma vez que faz uso da mesma para fornecer assistência em dinheiro direto, nomeadamente em campos de refugiados na Jordânia.[215] Além disso, outro exemplo do uso da *Blockchain* é a eficácia que tem na ajuda em entrega de bens alimentares a mais de 106.000,00 refugiados em diferentes países.[216] O programa *World Food Programm* desenvolvido pelas Nações Unidas está a trabalhar ativamente para estabelecer uma arquitetura de *blockchain* mais ampla, capaz de impulsionar o futuro da administração e fornecimento de operações em cadeia mais eficazes e céleres.[217] Ademais, o programa

---

208 Michael J.W. Rennock, Alan Cohn, Jared R. Butcher, *Blockchain Technology and Regulatory Investigators,* https://www.steptoe.com/images/content/1/7/v3/171269/LIT-FebMar18-Feature-Blockchain.pdf, 2018, p. 36.
209 Ibidem.
210 Ibidem.
211 Ibidem.
212 Marco André da Silva Costa, Abdelhamid Nedzhad, Danijela Lucic, *Designing a Digital Education Ecosystem,* https://www.researchgate.net/profile/Venelin-Terziev/publication/351956534_DESIGNING_A_DIGITAL_EDUCATION_ECOSYSTEM/links/60b21574a6fdcc1c66ec67a0/DESIGNING-A-DIGITAL-EDUCATION-ECOSYSTEM.pdf#page=152, 2021 p. 148.
213 Ibid…, p. 149.
214 Ibidem.
215 Ibidem.
216 Ibidem.
217 Ibidem.

tem testado a *Blockchain* como forma de tornar as transferências de dinheiro de apoio humanitário mais transparentes e seguras, para que possam ajudar mais famílias a sair do desespero.[218]

Mas como é que se tramita esse processo? A ideia é que os utilizadores comprem mercadoria em determinadas lojas, dependendo da função que lhes é atribuída, procedendo ao pagamento através de um *QR code* que é único e especifico para cada utente, identificando o cliente e informando-o de quanto saldo lhe resta.[219] O único local onde já foi testado este método foi a Jordânia, onde à primeira vista parece facilitar a capacidade de ajuda humanitária por parte das Nações Unidas, no entanto, o seu objetivo final é que não haja restrição a nível de compra e que os utilizadores possam usar esse dinheiro em qualquer que seja a sua necessidade, dentro dos campos de refugiados.[220]

Independentemente dos problemas preocupantes que a humanidade tem vindo a transpor, a verdade é que está também a passar por um período excecional a nível tecnológico. Assim, a combinação da *Blockchain* com investimentos por parte de sujeitos internacionais pode desempenhar um papel altamente relevante na realização dos Objetivos de Desenvolvimento Sustentável por parte da ONU, contribuindo para o bem-estar social mundial, e combatendo problemas como a pobreza extrema, a fome, e problemas ambientais. Isto significa que a mudança deixa de estar nas mãos dos grandes dirigentes das organizações internacionais, passando a estar do lado dos cidadãos comuns, permitindo que cada um de nós tenha impacto na sociedade global e no bem-estar dos ecossistemas em que habitamos.

Além disso, as redes sociais além de terem um impacto significativo na vida dos sujeitos singulares, também têm na vida dos grandes sujeitos coletivos, tais como as Organizações Internacionais, permitindo-lhes fazer chegar informação aos cidadãos de forma célere e eficaz.

11. O Regime Jurídico Internacional contra os Ciberataques

[218] Ibid…, p. 150.
[219] Ibidem.
[220] Ibid…, p. 151.

11.1. Ciberterrorismo e *jus ad bellum*

Os governos de hoje estão cientes da vulnerabilidade das suas infraestruturas domésticas e da ameaça potencial que é o ciberterrorismo. E enquanto estes ciberataques são cada vez mais comuns e cada vez mais complexos, o mesmo não se pode comentar acerca da cooperação entre os Estados.

Por exemplo, aquando do relatório feito pela CTITF no que toca a ameaças preocupantes para os países, apenas 2 levantaram essa questão. Algo que contradiz o facto de tantos países como os EUA, a China, Rússia, Irão, RU e Israel estarem a desenvolver as suas capacidades de cibersegurança e ciberataque tão rapidamente.[221]

Os Estados são sujeitos de direito internacional, o que significa que podem dividir-se em duas categorias: os estados soberanos e os estados com soberania limitada, onde se inserem os Estados protegidos, vassalados, exíguos, confederados, ocupados e divididos. O Estado é uma pessoa coletiva, apresenta-se como uma comunidade política organizada, que exerce determinada autoridade sobre um território, é um conjunto de órgãos que prosseguem essas diversas atividades. Como formula Marcelo Rebelo de Sousa, ‘’um povo fixado num determinado território, que institui por vontade própria, dentro desse território, um poder politico relativamente autónomo’’.[222] O Estado compreende, por isso, três elementos fundamentais: o seu povo, o seu território e o seu poder político.

Mas a demonstração de soberania de um Estado releva três direitos:

- O direito de elaborar tratados – *Ius Tractuum*;
- O direito de receber e enviar representantes diplomáticos – *Ius Legationis*;
- O direito de ‘’fazer a guerra’’ – Ius Bellium, conceito este que foi revolucionado, tendo agora o interprete de o ler de forma atualista de acordo com o n.º 4 do artigo 2.º da CNU, sendo então considerado este direito como legitima defesa individual ou coletiva, só assim sendo permitido o uso da força.

Este último direito é o mais relevante para a questão que aqui se coloca relativamente à possibilidade de um direito internacional capaz de combater os ataques

---

[221] Yaroslav Shirkyaev, Cyberterrorism in the Context of Comtemporary International Law, https://digital.sandiego.edu/cgi/viewcontent.cgi?article=1077&context=ilj, p. 173.

[222] Revista Militar, Major Reinaldo Saraiva Hermenegildo, Estado de Soberania: que paradigma?, https://www.revistamilitar.pt/artigo/74.

ciberterroristas. Há doutrina que defende que um Estado só pode ‘’acionar’’ o direito de autodefesa quando existe um ataque armado, a contracorrente defende que não e que, por isso, é possível acionar esse mecanismo aquando dos ataques ciberterroristas.[223]

A meu ver, parece-me pouco pertinente dizer que é possível agir em autodefesa armada aquando de um ataque ciberterorrista tendo em conta o facto de que a maioria dos ataques cibernéticos e terroristas são feitos anonimamente, ao contrário dos ataques terroristas tradicionais, e acaba por ser extremamente difícil ‘’apontar o dedo’’ especificamente a um governo ou organização, quando pode ter sido apenas uma pessoa a conduzir o ataque. É por isso que é extremamente difícil reagir a estes ataques proporcionalmente tal como a lei internacional manda.

Regra geral, o ciberterrorismo exige uma reinterpretação da necessidade e proporcionalidade sob uma nova visão. Os Estados não vão ser apenas obrigados a apresentar provas claras e convincentes da necessidade de usar força legitima em defesa de atos que não são propriamente e facilmente rastreáveis, como também têm de explicar porque razão deverão escolher o meio armado, se vão atacar com forças militares pessoas que provavelmente nunca seguraram sequer uma arma na vida.[224] Finalmente, é pertinente, também, observar que o ‘’fator sorte’’ elimina a distinção entre preempção e prevenção no que toca à legitima defesa antecipada, desde que a certeza de que irá ocorrer um ataque se torna impossível de prever, já que a rapidez com que se pode formar um ataque cibernético, a falta de necessidade de meios humanos e armamento o torna um ataque surpresa. Podemos concluir, por isso, que só será possível que um estado aja contra outro sujeito internacional caso haja suspeita de ciberataque, se houver um aumento na magnitude dos ciberataques, atingindo o nível de ataque armado com o próximo que se avizinha, ou enão se houver uma série de ataques cibernéticos tão devastadores e idênticos que se torna possível prever qual é o próximo na lista.

11.2. A Convenção do Conselho da Europa sobre Cibercrime

Apesar do empenho da comunidade internacional, como foi supramencionado, até agora não há um instrumento internacional especificamente para o combate ao terrorismo

[223] Yaroslav Shirkyaev, *Cyberterrorism in the Context of Comtemporary International Law*, https://digital.sandiego.edu/cgi/viewcontent.cgi?article=1077&context=ilj, p. 174.
[224] Ibid..., p. 180.

tradicional, muito menos para o terrorismo cibernético. Ainda assim, existem leis e atos normativos que regulamentam parcialmente esse problema, havendo obrigação de todos os signatários a aderir e respeitá-los.[225]

A questão da cooperação internacional no combate ao cibercrime foi discutida no XII Congresso das Nações Unidas, onde foi discutida a prevenção do crime e a justiça criminal internacional.[226] A UNODC, num documento preparado antes do Congresso, sugeriu que fosse preparada uma convenção abrangente contra os crimes cibernéticos, que deviam receber atenção especial. A América Latina e as Caraíbas eram a favor dessa ideia, enfatizando a necessidade do desenvolvimento de uma convenção internacional sobre crimes cibernéticos.[227] Além disso, a UNODC também pediu especial atenção para o facto de os crimes cibernéticos e os ataques terroristas de alta complexidade serem dotados de uma natureza transnacional, fazendo com que as questões de soberania nacional de cada país possam dificultar investigações criminais na ausência de cooperação ativa entre a lei e as agências de execução das jurisdições envolvidas.[228]

Atualmente, as principais convenções internacionais que discutem e tratam o crime cibernético é a Convenção do Conselho da Europa sobre Cibercrime, que foi assinada em Budapeste em 2001 e entrou em vigor em 2004.[229]

Embora a Convenção tenha sido redigida sob os auspícios do Conselho da Europa, está aberto à assinatura de países não membros, sendo que dos não membros, já quatro assinaram a Convenção: EUA, Canadá, Japão e África do Sul.[230] A Convenção inclui uma série de crimes pelos quais os Estados signatários são obrigados a implementar na sua legislação nacional, incluindo *hacking*, pornografia infantil, outros delitos e uma série de trabalhos que tratam da violação de propriedade intelectual.[231] Além disso, estabelece uma série de mecanismos processuais que os signatários devem, também, implementar no país, incluindo a atribuição de poderes de aplicação da lei na internet às autoridades,

---

[225] Enver Buçaj, *The Need for Regulation of Cyber Terrorism Phenomena in Line With Principles of International Criminal Law,* 2017, p. 143.
[226] Ibid..., p. 144.
[227] Ibidem.
[228] Ibidem.
[229] Ibid..., p. 145.
[230] Ibidem.
[231] Ministério Público Portugal, *Convenção sobre o cibercrime,* https://www.ministeriopublico.pt/instrumento/convencao-sobre-o-cibercrime-0.

por forma a monitorizar as atividades criminosas no mundo digital.[232] A Convenção convida, por isso, os signatários a cooperarem em maior medida no desenvolvimento da investigação e repressão de infrações relativas a cibercrime.

11.3. A importância da lei internacional regulamentar o cibercrime

Como não existe legislação que permita a prisão ou processo contra os criminosos no mundo digital, estes irão ser sempre uma ameaça omnipresente à saúde financeira das empresas, à privacidade dos seus clientes, e uma crescente ameaça à segurança de países e nações.

A verdade é que os agentes de execução não podem agir contra criminosos que não sabem ao certo quem são, e também devido ao facto de muitos dos países que são atacados por este tipo de crime não aplicarem as leis que criminalizam atividades em que outros países criminosos estão envolvidos em crimes cibernéticos.

O maior problema que se coloca na feitura de uma legislação internacional capaz de combater o crime cibernético está no facto de cada país ter um nível de desenvolvimento tecnológico diferente. O ciberterrorismo é uma ameaça e um desafio a nível nacional, comunitário e internacional, independentemente do facto de as partes interessadas reconhecerem a ameaça que é. A dificuldade está em definir as leis que são necessárias para viabilizar a captura e repressão de criminosos informáticos. E embora pareça uma tarefa relativamente simples, aqui são levantadas questões muito complicadas. Uma delas é se o alcance da definição de leis de cibercrime e ciberterrorismo devem incluir apenas aquelas que proíbam atividades que visam computadores ou a necessidade de proibir crimes contra dispositivos que também tenham sido corrompidos através de *tracking online*.[233]

Ao contrário do terrorismo e do crime tradicionais, o cibercrime e o ciberterrorismo são crimes globais. Crimes que atingem dispositivos em todos o mundo, ocorrendo no espaço cibernético que não vê os limites convencionais dos Estados.

Numa altura em que o mundo começa lentamente a lidar com a fronteira transnacional, legislação e jurisprudência tornam-se muito contraditórias.

---

[232] Ibidem.

[233] Enver Buçaj, *The Need for Regulation of Cyber Terrorism Phenomena in Line With Principles of International Criminal Law,* 2017, p. 148.

12. Considerações finais

Independentemente dos problemas preocupantes que a humanidade tem vindo a transpor, a verdade é que está também a passar por um período excecional a nível tecnológico.

A principal conclusão que podemos retirar daqui é que a tecnologia e o digital têm um poder imenso que, quando em mãos erradas, pode levar a situações extremas e perigosas para as relações internacionais. É por isso que é de extrema importância estudar como funcionam as plataformas digitais, saber lidar com elas e ter atenção àquilo que permitimos que elas tenham acesso diariamente. Tudo aquilo que colocamos na internet uma vez, fica para sempre nela guardado.

O futuro das relações internacionais depende em grande parte do futuro da cibersegurança. Como podemos verificar ao longo da dissertação, a cibersegurança é uma necessidade premente para que seja possível manter seguros aqueles que podem ser segredos de estado, economias nacionais e relações interestatais. No entanto, o maior problema que se coloca é o facto de a maioria dos cibercrimes ocorrerem por agentes anónimos, sendo cada vez mais difícil conseguir rastrear tanto quem os pôs em prática, como o país de onde originaram. Ao contrário de um ataque terrorista comum, um ciberataque não permite que vejamos a cara de quem o leva a cabo. O ciberterrorismo tem a facilidade de não necessitar de mais do que um computador e uma pessoa para o colocar em ação. Não necessita de qualquer armamento, nem de grandes gastos económicos e, por consequência, é praticamente impossível de punir aqueles que o praticam.

É por isso que é de extrema importância que se faça um esforço internacional de cooperação no sentido da criação de uma legislação transnacional, capaz de prever e punir estas situações, sem que esse fardo recaia sobre os países na sua jurisdição. Enquanto não for feito esse esforço e criada essa jurisdição internacional, não haverá forma efetiva de condenar ataques cibernéticos em larga escala, já que cada país é dotado de capacidades tecnológicas diferentes.

BIBLIOGRAFIA

1. Fontes Primárias

1.1. Fontes primárias impressas

Bjola, C.; Zaiotti, R. (2021) *Digital Diplomacy and International Organisations: Autonomy, Legitimacy and Contestation*. New York: Routledgle, (pp. 103-105).

Moslemzadeh Tehrani, P. (2017) *Cyberterrorism – The Legal and Enforcement Issues.* London: World & Scientific College Press, (pp. I a V).

P. Schimid, A.; J. Jongman, A. (1984) *Politicial Terrorism. A guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature.* Amsterdam: North-Holland Publishing Company, (pp. 28-32).

Wylie, C. (2019) *Inside Cambridge Analytica's Plot to Break the World.* United Kingdom: Profile Books, (pp. 76-78).

1.2. Fontes primárias *on-line*

Nações Unidas. (2014). Letter dated 27 June 2014 from the Permanent Representative of the Democratic People's Republic of Korea to the United Nations Addressed to the Secretary-General, A/68/934-S/2014/451. Disponível em: https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2014_451.pdf, data de consulta a: 25-04-2022.

Secretaria-Geral da Presidência do Conselho de Ministros. Regulamento Geral de Proteção de Dados. Disponível em: https://www.sg.pcm.gov.pt/sobre-nos/regulamento-geral-de-prote%C3%A7%C3%A3o-de-dados.aspx, data de consulta a: 17-06-2022.

White House. (2017). Statement by President Trump on The Paris Climate Accord. Disponível em: https://www.whitehouse.gov/briefings-statements/statement-president-trump-paris-climate-accord/, data de consulta a: 15-11-2021.

WhiteHouse. (2020). Remarks by President Trump in Press Briefing. Disponível em: https://www.whitehouse.gov/briefings-statements/remarks-president-trump-press-briefing/, data de consulta a: 15-11-2021.

2. Obras e artigos impressos

A. Baldwin, D. (2016). *Power and International Relations: A Conceptual Approach.* Estados Unidos: Princeton University Press, (p. 2).

Arquilla, J.; Ronfeldt, D. (2001). *Networks and Netwars: The Future of Terror, Crime and Militancy*. California: RAND, National Defense Research, (pp. 239-240).

Baezner, M.; Robin, P. (2017). *Stuxnet.* Zurique: Center for Security Studies, (p. 8).

Berghel, H. (2018). *Malice Domestic: The Cambridge Analytica Dystopia*. Las Vegas: University of Nevada, (p. 84).

Colarik, A. (2015). *Cyber Terrorism: Political and Economic Implications*. London: Idea Group Publishing, (p. xi).

DeSimone, A.; Horton, N. (2017). *Sony's Nightmare Before Christmas.* Baltimore: The Johns Hopkins University Applied Physics Laboratory, (p. 14).

Goodman, S. (2003). *Toward a treaty-based international regime on cyber crime and terrorism.* Washington D.C.: Center for Strategic and International Studies Press, (pp. 65-78).

K. Mulligan, D.; B. Schneider, F. (2011). ''Doctrine for Cybersecurity'', Dædalus, the Journal of the American Academy of Arts & Sciences, 1 de outubro: 11.

Nagy, V. (2012). *The geostrategic struggle in cyberspace between the United States, China, and Russia*. Budapeste: National University of Public Services, (p. 23).

3. Webgrafia

3.1. Artigos, relatórios e outros documentos

Bey, M., (2022) *Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition*. Disponível em: https://www.jstor.org/stable/pdf/26554994.pdf?refreqid=excelsior%3A1f5b47051680b7cc1e3f81001ca31d2b&ab_segments=&origin=&acceptTC=1, data de consulta a 25-09-2022.

Buçaj, E. (2017). *The Need for Regulation of Cyber Terrorism Phenomena in Line With Principles of International Criminal Law* https://journals.univ-danubius.ro/index.php/juridica/article/view/3882/4033

Da Silva Costa, M.; Nezdzhad, A.; Lucic, D. (2021) *Designing a Digital Education Ecosystem.* Disponível em: https://www.researchgate.net/profile/Venelin-Terziev/publication/351956534_DESIGNING_A_DIGITAL_EDUCATION_ECOSYSTEM/links/60b21574a6fdcc1c66ec67a0/DESIGNING-A-DIGITAL-EDUCATION-ECOSYSTEM.pdf#page=152, data da consulta a 11-02-2022.

Harvard Kennedy School, Shorenstein Center on Media, Politics and Public Policy (2012) *Social Media used by regime and activists in Syrian Revolution, says NPR's Deborah Amos*. Disponível em: https://shorensteincenter.org/speaker-series-with-nprs-deborah-amos/, data de consulta a 22-06-2022.

IISS (2021) *Cyber Capabilities and National Power: A Net Assessment, Research Papers*. Disponível em: https://www.iiss.org/-/media/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---united-states.pdf, data de consulta a 04-06-2022.

J.W. Rennock, M.; Cohn, A.; R. Butcher, J. (2018) *Blockchain Technology and Regulatory Investigators*. Disponível em: https://www.steptoe.com/images/content/1/7/v3/171269/LIT-FebMar18-Feature-Blockchain.pdf, data de consulta a 12-07-2022.

Knowledge at Wharton, (2019) *Why Social Media Is the New Weapon in Modern Warfare*, Warton University. Disponível em: https://knowledge.wharton.upenn.edu/article/singer-weaponization-social-media/, data de consulta a 27-08-2022.

Kushner, D., (2013) *The Real Story of Stuxnet*, Duke University. Disponível em: https://courses.cs.duke.edu/spring20/compsci342/netid/readings/cyber/stuxnet-ieee-spectrum.pdf, data de consulta a 11-12-2021.

Langlois, L., (2018) *Trump, Brexit and the Transatlantic Relationship: The New Paradigms of Trump Era.* Disponível em: https://www.journals.openedition.org/lisa/10235, data de consulta a 15-01-2022.

Lynch, M.; Freelon, D.; Aday, S. (2012) *Syria's Socially Mediated Civil War,* United States Institute of Peace. Disponivel em: https://www.usip.org/sites/default/files/PW91Syrias%20Socially%20Mediated%20Civil%20War.pdf, data de consulta a 14-03-2022.

Mallick, PK. (1999) *Internet – A Weapon of War*, The Centre for Land Warfare Studies. Disponível em: https://www.researchgate.net/publication/344737617, data de consulta a 28-08-2022.

M. Martin, D. (2016) *Tracing the Lineage of DarkSeoul,* SANS Institute. Disponível em: https://www.sans.org/reading-room/whitepapers/critical/tracing-lineage-darkseoul-36787, data de consulta a 15-08-2022.

Parjis, D.; Shapiro, J. (2017) *The transatlantic meaning of Donald Trump: a US-EU Power Audit*, European Council on Foreign Relations. Disponível em:

https://ecfr.eu/publication/the_transatlantic_meaning_of_donald_trump_a_us_eu_power_audit7229/,21, data de consulta a 07-09-2021.

Pothier, F.; Vershbow, A. (2017) *NATO and Trump The Case for a New Transatlantic Bargain*, Atlantic Council, Brent Scowcroft Center on International Security. Disponível em: https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/NATO_and_Trum p_web_0623.pdf, data de consulta a 15-09-2021.

Prestes, E. (2019) *An Overview of the United Nations High-Level Panel on Digital Cooperation*. Disponível em: https://www.researchgate.net/publication/331664721_An_Overview_of_the_United_Nations_High-Level_Panel_on_Digital_Cooperation_Industry_Activities, data de consulta a 19-10-2021.

Robinsons, K. (2021) *What is the Iran Nuclear Deal?,* Council on Foreign Relations. Disponível em: https://www.cfr.org/backgrounder/what-iran-nuclear-deal, data de consulta a 13-05-2022.

Saraiva Hermenegildo, R. (2004) *Estado de Soberania: que paradigma*?, Revista Militar. Disponível em: https://www.revistamilitar.pt/artigo/74, data de consulta a 25-08-2022.

Shirkyaev, Y. (2012) *Cyberterrorism in the Context of Comtemporary International Law*. Disponível em: https://digital.sandiego.edu/cgi/viewcontent.cgi?article=1077&context=ilj, data de consulta a 28-08-2022.

S. Nye, J. (2010) *Cyber Power*, Harvard Kennedy School. Disponível em: https://apps.dtic.mil/sti/pdfs/ADA522626.pdf, data de consulta a 17-06-2021.

Vaughan-Nichols, S. (2018) *How Cambridge Analytica used your Facebook Data to help elect Trump,* Networking. Disponível em: https://www.zdnet.com/article/how-

cambridge-analytica-used-your-facebook-data-to-help-elect-trump/, data de consulta a 13-01-2022.

Weimann, G. (2004) *How Real is the Threat?*, United States Institute of Peace. Disponível em: https://www.usip.org/sites/default/files/sr119.pdf, data de consulta a 09-12-2021.

3.2.Websites consultados

Arms Control Association, *Timeline of Nuclear Diplomacy With Iran*. Disponível em: https://www.armscontrol.org/factsheets/Timeline-of-Nuclear-Diplomacy-With-Iran, data de consulta a 15-05-2022.

Australian Human Rights Commission, *What is the Universal Declaration of Human Rights?*. Disponível em: https://humanrights.gov.au/our-work/what-universal-declaration-human-rights, data de consulta a 22-10-2021.

Britannica, *History of Technology*. Disponível em: https://www.britannica.com/technology/history-of-technology, data de consulta a 10-04-2021.

Britannica, *Kosovo Conflict*. Disponível em: https://www.britannica.com/event/Kosovo-conflict, data de consulta a 17-08-2022.

Business Insider, *Experts: The Sony Hack Looks a Lot Like Previous Attacks on South Korea*. Disponível em: www.businessinsider.com/experts-say-sony-hack-looks-a-lot-like-previous-attacks-on-south-korea-2014-12, data de consulta a 14-08-2022.

CISCO, *What is Cybersecurity*? Disponível em: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html, data de consulta a 13-07-2022.

Deadline, *The Sony Hack One Year Later: Just Who Are The Guardians of Peace?*. Disponível em: https://deadline.com/2015/11/sony-hack-guardians-of-peace-one-year-anniversary-1201636491/, data de consulta em: 03-06-2022.

Digwatch, *The UN High-Level Panel on Digital Cooperation.* Disponível em: https://www.dig.watch/processes/hlp, data de consulta a 09-11-2021.

DiscoverTec, *The Evolution of Technology: Past, Present and Future.* Disponível em: https://www.discovertec.com/blog/evolution-of-technology, data de consulta a 11-04-2021.

European Comission, *What is personal data.* Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en, data de consulta a 27-11-2021.

FactCheck, *FactChecking Trump's Attack on the WHO.* Disponível em: https://www.factcheck.org/2020/04/factchecking-trumps-attack-on-the-who/, data de consulta a 12-10-2021.

Fortune, *Inside the Hack of the Century. Part 2: The Storm Builds*. Disponível em: https://www.fortune.com/sony-hack-part-two/, data de consulta a 14-08-2022.

Frontline, *A Kosovo Chronology*. Disponível em: https://www.pbs.org/wgbh/pages/frontline/shows/kosovo/etc/cron.html, data de consulta a 10-09-2022.

History, *The Space Race*. Disponível em: https://www.history.com/topics/cold-war/space-race, data de consulta a 18-09-2022.

Human Rights Watch, *What are Human Rights?*. Disponível em: https://www.hrw.org/news/2014/09/15/what-are-human-rights, data de consulta a 06-08-2022.

IISS, *CyberPower – Tier One*. Disponível em: https://www.iiss.org/blogs/research-paper/2021/06/cyber-power---tier-one, data de consulta a 07-09-2021.

Internal Results, *The Complete Guide to Content Personalization.* Disponível em: https://www.internalresults.com/resources/content-personalization, data de consulta a 08-12-2021.

ITGovernance, *What is Cybersecurity? Definition and Best Practices*. Disponível em: https://www.itgovernance.co.uk/what-is-cybersecurity, data de consulta a 12-04-2022.

Ministério Público Portugal, *Convenção Sobre o Cibercrime*. Disponível em: https://www.ministeriopublico.pt/instrumento/convencao-sobre-o-cibercrime-0, data de consulta a 07-09-2022.

NASA, *Explorer and Early Satellites*. Disponível em: https://www.nasa.gov/mission_pages/explorer/explorer-overview.html, data de consulta a 25-02-2022.

NASA, *NASA History*. Disponível em: https://www.nasa.gov/topics/history/index.html, data de consulta a 23-02-2022.

New York Times, *More Sanctions on North Korea after Sony Case*. Disponível em:https://www.nytimes.com/2015/01/03/us/in-response-to-sony-hack/2014/12/22/b76fa0a0-8a1d-11e4-9e8d-0c687bc18da4_story.html, data de consulta a 14-05-2022.

NITAAC, *The Importance of Technologies in Government*. Disponível em: https://nitaac.nih.gov/resources/articles/importance-cyber-technologies-government, data de consulta a 17-07-2022.

Norton, *What is cybersecurity? What you need to know*. Disponível em: https://us.norton.com/blog/malware/what-is-cybersecurity-what-you-need-to-know#, data de consulta a 06-09-2022.

Oxford Reference, *Applied Arts*. Disponível em: https://www.oxfordreference.com/view/10.1093/oi/authority.20110803095420946, data de consulta a 12-04-2021.

Reuters, *Sony Hires Mandiant after cyber attack, FBI starts probe*. Disponível em: www.reuters.com/article/us-sony-cybersecurity-mandiant/sony-hires-mandiant-after-cyber-attack-fbi-starts-probe-idUSKCN0JE0YA20141201, data de consulta a 17-06-2022.

SDG Knowlege Hub, *UN High-Level on Digital Cooperation Calls for 2020 Global Commitment.* Disponível em: https://sdg.iisd.org/news/un-high-level-panel-on-digital-cooperation-calls-for-2020-global-commitment/, data de consulta a 14-04-2022.

SOS Can Help, *How does Antivirus work*. Disponível em: https://www.soscanhelp.com/blog/how-does-antivirus-work#what, data de consulta a 16-08-2022.

Technica, *Facebook's Cambridge Analytica Scandal, Explained.* Disponível em: www.arstechnica.com/tech-policy/2018/03/facebooks-cambridge-analytica-scandal-explained, data de consulta a 12-10-2021.

The Economist, *George Bush and the axis of evil*. Disponível em: https://www.economist.com/leaders/2002/01/31/george-bush-and-the-axis-of-evil, data de consulta a 14-06-2022.

The Guardian, *Cambridge Analytica: how did it turn clicks into votes?*. Disponível em: https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes- christopher-wylie, data de consulta a 12-10-2021.

The Guardian, *What is Cambridge Analytica?*. Disponível em: https://www.theguardian.com/news/2018/mar/18/what- is-cambridge-analytica-firm-at-centre-of-facebook-data-breach, data de consulta a 13-10-2021.

The Hacker News, *The Syrian spyware to targe the opposition activists*. Disponível em: https://thehackernews.com/2012/02/syrian-spyware-to-target-opposition.html, data de consulta a 19-09-2022.

The Nation, *History and Evolution of Technology*. Disponível em: https://www.nation.com.pk/23-Jul-2018/history-and- evolution-of-technology, data de consulta a 15-04-2021.

The Washington Post, *Is Russia or China The Biggest Cyber Threat? Experts are Split.* Disponível em: https://www.washingtonpost.com/politics/2022/01/20/is-russia-or-china-biggest-cyber-threat-experts-are-split/, data de consulta a 08-08-2022.

The Washington Post, *The Cybersecurity 202: The United States is still number one in cyber capabilities*. Disponível em: https://www.washingtonpost.com/politics/2021/06/28/cybersecurity-202-united-states-is-still-number-one-cyber-capabilities/, data de consulta a 14-09-2022.

The Washington Post, *Stuxnet was work of U.S. and Isreali experts, officials say*. Disponível em: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html, data de consulta a 07-08-2022.

The Washington Post, *The Sony Pictures hack, explained.* Disponível em: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/, data de consulta a 06-07-2022.

The World Bank, *Islamic Republic of Iran*. Disponível em: https://www.worldbank.org/en/country/iran/overview, data de consulta a 04-08-2022.

United Nations, *Civil Society*. Disponível em: https://www.un.org/en/civil-society/secretary-general's-high-level-panel-digital-cooperation, data de consulta a 17-04-2022.

U.S. Cyber Command, *Our History*. Disponível em: https://www.cybercom.mil/About/History/, data de consulta a 12-09-2022.

Vanity Fair, *An Exclusive Look at Sony's Hacking Saga*. Disponível em: https://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg, data de consulta a 19-08-2022.

Varsity, *Who is Dr. Aleksandr Kogan, the Cambridge Academic Accused of Misusing Facebook Data?*. Disponível em: www.varsity.co.uk/news/15192, data de consulta a 05-04-2021.

Wired, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*. Disponível em: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/, data de consulta a 07-08-2022.

Your Europe, *A proteção de dados ao abrigo do RGPD.* Disponível em: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pt.htm#shortcut-1, data de consulta a 15-09-2022.

UNIVERSIDADE DOS AÇORES
Faculdade de Ciências Sociais e Humanas

Rua da Mãe de Deus 9500-321 Ponta Delgada
Açores, Portugal