Da Espionagem à Ciberespionagem

Inês Rodrigues Oliveira

Resumo: A era informática, trouxe ao mundo uma nova realidade e uma vasta gama de preocupações. Contudo, as motivações e as práticas antigas não deixaram de existir, algumas até evoluíram e tornaram os seus resultados mais promissores.

Imagine-se, por exemplo a espionagem, uma prática existente desde a era A.C. que aplicada aos tempos de hoje e aliada à tecnologia cria um novo termo a ciberespionagem.

Sun Tzu [1] considerava que a espionagem e os espiões eram um meio importante na guerra, nos tempos de hoje essa guerra é no ciberespaço, *cyberwar*.

1. Introdução

Nem sempre a humanidade foi justa, ou é justa, desde os primórdios que ter vantagem, seja sobre outros países, empresas ou outras pessoas é considerado uma vitória. Muitas vezes, o custo dessa vitória é conseguir tirar informação privilegiada e ou mesmo segredos de estado de um país, a essa técnica dá-se o nome de espionagem.

De facto, a espionagem requer mais do que um mero acesso a documentos, é necessária habilidade, inteligência, foco, concentração, estudo, entre outras capacidades que o espião deverá adquirir.

Atualmente a evolução tecnológica elevou o patamar da espionagem para algo muito mais superior, a ciberespionagem.

Considera-se a ciberespionagem como o uso aprofundado de tecnologia para obter de outrem informação secreta, sem a sua permissão e ou consentimento. A obtenção deste tipo de informação tal como na espionagem será útil para conquistar vantagem sobre os rivais, governos, inimigos, vantagem pessoal, económica e política. Nestas duas práticas podem ser usados métodos da internet, das redes, de servidores *proxy*, técnicas da *cracking, hacking* entre outros.

A evolução da espionagem com o avanço tecnológico, constituem ainda um fenómeno alarmista e de grande impacto na sociedade, fenómeno este que cada país deve colmatar e controlar da forma mais viável e segura.

2. Espionagem vs. Ciberespionagem

2.1. Espionagem

De acordo com o SIS (Serviço de Informações de Segurança), "a espionagem consiste na obtenção de informação que, pelo seu valor e relevância para o interesse nacional, está protegida por medidas de segurança." [2]

No entanto, a definição de espionagem não se deverá restringir a informações nacionais e não públicas, apesar de se saber que estas informações consideradas classificadas de âmbito nacional poderão prejudicar as relações com outros países, e até mesmo a tomada de algumas decisões.

Como tal deveremos ter em consideração que a espionagem poderá acontecer no âmbito comercial, político e militar, com motivações diferentes, mas com objetivo final e igual, a obtenção de vantagem sobre o adversário [3].

O processo de espionagem requer meios técnicos e recursos humanos. O espião deverá ter duas faces, deve conseguir dissuadir e persuadir o outro de forma a obter a informação, isto é, um ato de espiar, seguir ocultamente e não deixar rasto.

Esta obtenção de informação secreta de forma clandestina é no ordenamento jurídico português

considerado como um crime punido de acordo com o artigo 317.º do Código Penal [4] , e controlado pelo SIS que de acordo com o artigo 3.º n.º 3 da Lei Orgânica 9/2007 [5], de 19 de Fevereiro, "O Serviço de Informações de Segurança (SIS) é o único organismo incumbido da produção de informações que contribuam para a salvaguarda da segurança interna e a prevenção da sabotagem, do terrorismo, a espionagem e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido."

2.2. Ciberespionagem

A ciberespionagem não tem ainda uma definição que seja possível usar, no entanto todas as possíveis definições consideram a ligação entre a espionagem e a tecnologia.

A ciberespionagem tem também o mesmo objetivo que a espionagem, isto é, ganhar vantagem sobre o adversário.

Por estas razões, e por ter o mesmo campo de batalha (político, comercial e militar), há quem considere a ciberespionagem uma variante tradicional da espionagem [6][7], uma exploração de vulnerabilidades para ter acesso à informação [8] ou mesmo uma atividade de inteligência [9].

O dicionário de Oxford considera a ciberespionagem como "o uso de redes de computadores para obter acesso ilícito a informações confidenciais, tipicamente que será realizada por um governo ou outra organização" [10] podemos também considerar a tecnologia como uma ferramenta complementar ao trabalho do espião.

Contudo é necessário explanar o que é efetivamente a ciberespionagem. O *Manual Tallinn* [11] é um documento académico sem poder vinculativo, que apela à resolução de ciberconflitos e dos direitos humanitários do Direito Internacional. A NATO esteve incluída como patrocinadora da sua opinião com o Centro de Excelência de Ciberdefesa Cooperativa, mas nunca tomou uma posição acerca deste manual. No manual é abordado uma definição que poderá mais tarde a vir a ser adotada, "qualquer ato praticado clandestinamente - o autor tenta esconder sua identidade- ou sob falsos pretexto - a sua intenção é a de apresentar-se como uma pessoa com direitos e autorização para aceder as informações alvo - que utiliza capacidades cibernéticas para obter (ou tentar obter) informações com a intenção de a transmitir à parte oponente do conflito." (Tallinn Manual, 2013)[11]

Pode-se considerar que a forma de ataque, isto é, a investida da ciberespionagem acontece de acordo com o acesso a serviços tecnológicos maliciosos que permitem a sabotagem [12] e roubo de informação [13] sem deixar qualquer rasto, muitas vezes num curto espaço de tempo.

Estas atuações podem ser motivadas e difundidas pelos *hackers* que na realidade são quem tem mais conhecimento quanto às práticas de cibercrime entre outras práticas maliciosas.

É importante salientar que todos os países têm um centro de ciberdefesa e cibersegurança, estas agências são responsáveis pela monitorização da prática da ciberespionagem.

Tendo estes atos como campo de batalha o chamado ciberespaço, o mais correto será não haver um único órgão responsável pela ciberespionagem, mas vários órgãos em conjunto. Como tal uma das entidades que monitoriza a Ciberespionagem é a DIRCSI – Direção de Comunicação e Sistemas de Informação do Estado Maior das Forças Amadas [14] [15], que atua em parceria com o Conselho Nacional de Cibersegurança [16].

Será pertinente referir que os direitos e a obrigações do Estado [17] [18] perante o seu povo, presentes na Constituição da República Portuguesa [19], baseiam-se na segurança e proteção dos mesmos, e por isso as questões de cibersegurança, ciberdefesa são fundamento de Segurança e Defesa do Estado [20].

Como foi dito anteriormente a ciberespionagem evoluiu da espionagem, então será que os requisitos se alteraram?

Será difícil precisar uma resposta concreta, contudo parece evidente que a única alteração que houve de requisitos foi o conhecimento avançado e especializado na área tecnológica e do ciberespaço.

O problema da ciberespionagem assenta tanto nos ciberconflitos como na ciberguerra, trás ao pensamento dos cidadãos a velha questão, "será que estamos efetivamente protegidos para o futuro que aí vem?"

2.3. A história

Compreender a história e a evolução da espionagem e ciberespionagem é dar um passo para perceber a problemática deste tema e o seu lado negro.

Como já foi várias vezes referido, desde os primórdios da humanidade que existe a arte de espiar, até nas cortes de toda a europa existiu espiões. Mas foi no século XX que a espionagem teve o seu auge, na II Guerra Mundial [21][22], foram criadas as primeiras agências de espionagem. Nos Estados Unidos da América criou-se a OSS (*Office of Strategic Services*) atualmente CIA (*Central Intelligence Agency*) [23], na União Soviética a NKVD mais tarde deu origem à KGB (*Komitet Gosudarstvennoi Bezopasnosti*) e por fim no Reino Unido foi criado o MI (*Military Intelligence*) que se dividiu em MI5 e MI6.

Todas estas agências tinham algo em comum para além da espionagem, o termo *intelligence,* "informações recolhidas por governos ou organizações para orientarem as suas decisões. Nela se incluem informações que podem ser tanto públicas como privadas, obtidas a partir de várias fontes, quer públicas, quer até secretas ou até da junção de ambas." [24]

A guerra fria veio reforçar a arte da espionagem, esta guerra só tinha uma forma de acabar, seria quando uma parte conseguisse obter e aceder de forma privilegiada a documentos e informações secretas do Estado adversário. Portanto, foi uma guerra extrema, sem precedentes onde a espionagem "*foi a chama da fogueira que ardia".*

Ainda durante esta guerra, vários acordos e alianças foram surgindo, uma delas foi a Aliança SIGINT ou Tratado de Segurança UK-USA (UKUSA) [25]. Esta Aliança SIGINT aconteceu no ano de 1946 com o objetivo de partilhar informação secreta, isto é, através da interseção de sinais, por exemplo descodificação de mensagens, principalmente trocada entre tropas Alemãs, Japónicas e Soviéticas. Faziam parte deste acordo a Austrália, Canadá, Nova Zelândia, Reino Unido e EUA, ao qual foram posteriormente apelidados *The Five Eyes* [26].

Sob este acordo nasceu ainda o sistema *Echelon* [27], que foi criado como sendo uma rede de vigilância global. Até ao ano de 2013 acreditava-se que esse sistema já teria desativado ou deixado de existir, contudo Edward Snowden [28], ex-administrador de sistemas da CIA e ex

contratado da NSA, rebentou com um escândalo admitindo que o mesmo continua ativo apresentando provas.

Ora a ser verdade será importante perceber que é um sistema de vigilância mas também um sistema de espionagem.

3. Os ciberataques e o seu impacto

A abordagem dos ciberataques de espionagem deverá incluir as dimensões e as suas repercussões no âmbito social.

Como João Moreira refere na sua investigação de 2012 um ciberataque é "(…) um ataque lançado geralmente a partir de um computador recorrendo ao método de intrusão e tem como finalidade adquirir, explorar, perturbar, romper, negar, degradar ou destruir informação constante em computadores ou em redes de computadores, em sistemas e equipamentos eletrónicos ligados a outros equipamentos ou sistemas ou que partilham a mesma estrutura de energia ou o mesmo espaço de emissão eletromagnética, bem como os próprios computadores, rede de computadores, sistema e equipamentos." [29]

No ano de 2003 o Instituto de Defesa Nacional fazia referência ao risco inerente dos ciberataques. No Caderno de Estratégia de Informação de Segurança do Ciberespaço, foram considerados várias formas de ataques cibernéticos: simples, organizados, APT, de grande escala coordenados e ataques físicos.[30]

O que mais se adequa pelas suas caraterísticas à ciberespionagem é os APT- *Advanced Persistent Threaths*. Estes ataques criados por hackers com elevada perícia tecnológica, permanecem como espiões no sistema por um longo período de tempo e ativam quando o controlador pretende.

A cada dia que passa estes riscos aumentam, a tecnologia evolui, estes crescem e tornam-se indestrutíveis. Mesmo que um ciberataque não seja APT, há três fases em comum com outros, primeira fase a identificação das vulnerabilidades sistemas e rede, segunda fase invasão da rede e inserção do malware e por fim, a terceira fase de eliminar as provas e os vestígios.

Vejamos alguns exemplos de ataques que abalaram as relações entre países, em 2003 o *"Titan Rain"*,[31] foi um ataque APT que terá influenciado a relação China-EUA, contudo em 2008 [32] esta relação voltou a ser afetada, suspeitas de que a China enviava documentos confidenciais aos adversários das candidaturas à presidência dos EUA. No entanto, nas últimas eleições dos EUA, e também de outras partes do mundo viu-se as influências de outros países usando técnicas cibernéticas e de ciberespionagem. [33][34]

Outro ataque que teve motivações políticas foi o ataque DOS- *Denial of Service*, [35] à Estónia em 2007 que abalou a relação com a Rússia.

Cinco grandes campanhas ligadas à ciberespionagem e aos ciberataques que surgiram nos anos 2009 a 2013 foram a GhostNet (2009) [36], Operação Aurora (2010) [37], Stuxnet (2011) [38], Flame (2012) [39] e Outubro Vermelho (2013) [40]. Estas cinco campanhas têm em comum a intrusão dos sistemas, o roubo de informação confidencial, a sabotagem do sistema, a perturbação dos sistemas e o abalo de relações diplomáticas.

Será relevante abordar o PRISM, [41] o maior sistema de ciberespionagem que permite a consulta do registo a chamadas, recolhe informação a partir de redes sociais, e é usado pela NSA para armazenar dados pessoais, dados institucionais, de governantes, de países aliados e não aliados.

A prática do cibercrime é uma matéria delicada, vejamos o que aconteceu nos Jogos Olímpicos de Inverno 2018 [42]. Um ataque paralisou a comunidade olímpica afetando essencialmente equipas como a Rússia, China e Coreia do Norte. Vários estudos afirmaram que terá havido intenções de ciberespionagem.

Para se ter uma perspetiva do futuro, novas campanhas e programas de ciberespionagem foram descobertos já no inicio de 2018, como o caso Finfisher*, Pallas, Skygofree*. [43]

Será impossível descrever todos os ataques que houveram até ao dia de hoje, os vários países deverão ter a consciência que cada dia que passa é um dia, em que uma campanha nova aparece, ou é mais um dia sob os olhos quem nos espia e nos controla.

3.1. Outras formas tecnológicas de espionagem

Existe ainda outras formas de espionagem, evoluídas de acordo com a sociedade atual.

Anteriormente, os espiões recorriam à caixa de fósforos onde traziam as informações escondidas, atualmente podem recorrer ao uso de *USB dread drop,*[44] uma forma inovadora em que a pen drive é colocada num local público escondida num muro de tijolos, e quem tiver acesso consegue fazer troca de documentos com o espião. O *dread drop* é composto por dois documentos: o dreapdrops-manifesto.txt e um arquivo readme.txt. Já é possível adaptar este sistema à *wi-fi*, *dread drop wi-fi*. [45]

Há ainda uma preocupação crescente quanto às IOT (*Internet Of Things*) e *SmartGrids*, entre outras grandes tecnologias inovadoras ainda em expansão. Como é do conhecimento geral as IOT e as *SmartGrids* constituem uma assistência pessoal aos cidadãos quase como controladoras dos seus utilizadores, contudo não será de todo totalmente isenta a estas situações uma vez que poderão ser vulneráveis a estes tipos de ataques e vítimas de espionagem. [46][47]

4. A necessidade de medidas de cibersegurança

A nível Europeu, todos os países têm o mesmo entendimento sobre o panorama da cibersegurança quanto à necessidade de fazer esforços na tentativa de ampliar a sua abrangência. A UE considera que para garantir um mercado único digital é necessário proteger o "novo petróleo da economia", os dados.

Face ao aumento significativo da criminalidade do ciberespaço, a Comissão Europeia propôs a criação de uma agência de cibersegurança mais forte, com base na já existente ENISA. Entendeu assim, que era necessário apelar ao reforço da cibersegurança e ao aumento da ciberresiliência em toda a UE.

Compreendeu, ainda, a reforma por exemplo da diretiva SRI, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação, e a criação de um acordo interinstitucional que entrou em vigor a 20 de Dezembro de 2017 que cria uma Equipa de Resposta a Emergências Informáticas (CERT-UE) permanente, que abrange todas as instituições e agências da UE.

Também para a OCDE e a ONU a matéria da cibersegurança levanta questões de segurança ao qual ambas as organizações apelam à adoção de medidas de cultura de segurança dos sistemas de informação e rede, mas tambem à manutenção da paz internacional e cibernética.

Não só na UE, mas também em outras organizações é visível esta preocupação quanto à ciberdefesa e cibersegurança. Por exemplo o Canadá anunciou um investimento avultado nesta área com objetivo de confiança do comércio eletrónico, com promoção e proteção

dos cidadãos online, e ainda apoio à proteção das novidades digitais.

Nos EUA os esforços estão concentrados também num reforço destas estruturas, em 2017 Donald Trump terá assinado uma ordem executiva que pretende melhorar, fortalecer e promover a segurança *cyber*.

Afirmou ainda, que juntos estes esforços, melhorariam e garantiriam um país mais seguro às ameaças do Séc.XXI.

A Austrália por exemplo, têm uma vasta gama de documentos online de apoio às empresas para implementarem medidas de segurança, e uma vasta gama de medidas do governo quanto à proteção do estado. É notório que a Austrália tem nos seus pontos principais de trabalho a cibersegurança.

Outros países poderiam ser aqui abordados, contudo sabemos que há países que não são imunes à prática de cibercrimes como a Rússia, a China, a Coreia do Norte entre outros.

4.1. Os desafios e as soluções

Os desafios que se colocam neste âmbito passam muito pela mudança de paradigma, cultura organizacional, adoção de medidas de segurança, dinamização de ações que permitam estar um passo à frente dos agentes intrusos, e ainda o controlo do risco através da prática de auditorias.

Será importante dotar, por exemplo os funcionários de uma empresa, para que estes tenham consciência do risco associado às tecnologias, explicar o funcionamento da proteção dos computadores e capacitar para a segurança dos meios informáticos da empresa. É necessário criar políticas de tecnologia, adotar medidas que disciplinem o uso de dispositivos móveis e outros pessoais, e que possam por em risco a segurança de uma empresa.

Por fim e não menos importante, a importância da existência de um responsável pela segurança permanente das infraestruturas críticas da empresa. [48]

Estas e outras medidas poderão ser encontradas em alguns relatórios (ENISA [49], CNCS [50] e CERT'S (Equipa de Resposta a Emergências Informática Portuguesa)), e em outros relatórios não oficiais (Kapersky e Symantec), entre outros que fazem estudos aprofundados da cibersegurança.

5. Conclusão

Este artigo demonstra o essencial da evolução da espionagem até à ciberespionagem. Expõe a necessidade de um apoio internacional no combate a ciberespionagem, que como vimos pode ter consequências devastadoras, com riscos inimagináveis, por exemplo nas relações diplomáticas. O poder desta arte vai mais longe podendo alguns dos seus atos tornar-se em ciberconflitos e em atos de ciberterrorismo ou mesmo ciberguerra.

E, por isso muitas vezes foi explanado que tanto a espionagem como a ciberespionagem têm um objetivo comum, tomar vantagem sobre o país adversário, ou empresa adversária.

Outro facto aqui discutido foram as motivações e os objetivos dos ataques, como a obtenção de dados pessoais, a informação sigilosa, os benefícios económicos, as vantagens táticas a nível militar, as vantagens competitivas, as motivações políticas, a destruição, o dano e a vingança.

Contudo muitas mais ações de espionagem e ciberespionagem poderiam aqui ter sido expostas, no entanto a falta de acesso a informação fidedigna acaba por restringir a realidade dos ataques que podiam ter sido igualmente referenciados.

Por fim é necessário entender que estes atos não afetam só o estado em si, estes afetam todos nós, expõe-nos.

Há até quem diga, que hoje a guerra não se faz no terreno, mas sim no ciberespaço, e *"os dados são as balas do combate"*.

Referências

[1] TZU, Sun – A Arte da Guerra. Lisboa: Editorial Futura, 1974.

[2] https://www.sis.pt/ [Consultado a 1 de Março 2018]

[3] Silva, S. (2014). A Ciberespionagem no contexto português (Dissertação de Mestrado). Academia Militar, Lisboa.

[4] Código Penal - DL n.º 48/95, de 15 de Março

[5] Lei Orgânica Do Secretário-Geral Do SIRP, Do SIED e Do SIS - Lei Orgânica n.º 9/2007, de 19 de Fevereiro

[6] Militão, Octávio Pimenta. (2014). Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional (Dissertação de Mestrado). Faculdade de Ciências Sociais e Humanas - Universidade Nova de Lisboa, Lisboa.

[7] Leite, A. M. (2016). A problemática e os seus desafios. CEDIS working Papers, 49: (1-22)

[8] Santos, Daniela G. (2014). A Cibersegurança em Portugal: A ação política nacional em matéria de cibersegurança (Dissertação de Mestrado). ISCTE-Instituto Universitário de Lisboa, Lisboa.

[9] OLIVEIRA, S. B. - A Securitização do Cyber Space e Seus Desdobramentos para as Relações Internacionais. (Dissertação de Mestrado) – Faculdade de ASCES

[10]https://en.oxforddictionaries.com/definition/cyberespionage (consultado a 8 de Março de 2018)

[11] NATO Cooperative Cyber Defence Centre of Excellence, International Group of Experts at the Invitation - The Tallinn Manual on the International Law Applicable to Cyber Warfare – Cambridge University. 2013. [Consultado em 8 de Março 2018]. Disponível na Internet: https://issuu.com/nato_ccd_coe/docs/tallinnmanual

[12] Artigo 5.º Lei n.º 109/2009, de 15 de Setembro- Lei Do Cibercrime

[13] Artigo 6.º Lei n.º 109/2009, de 15 de Setembro- Lei Do Cibercrime

[14] EMGFA- Estado Maior General das Forças Armadas criação do DIRCSI- DL n.º 184/2014 de 29 de Dezembro. Disponível em: http://www.emgfa.pt/pt/organizacao/dircsi (consultado a 9 de Maio de 2018)

[15] Leite, A. M. (2016). A problemática e os seus desafios. CEDIS working Papers, 49: **(1-22)**

[16] DL n.º 69/2014, 9 de Maio Disponível em

[17] Lei n.º 53/2008 de 29 de Agosto- Lei da Segurança Interna

[18] Lei n.º 30/84 de 5 de Setembro – Lei quadro do Sistema de Informação da República Portuguesa

[19] Artigo 9.º e 27.º da Constituição da República Portuguesa

[20] IDN nação e defesa- cibersegurança n.º 133 (2008) Disponível em: https://www.idn.gov.pt/publicacoes/nacaodefesa/textointegral/NeD133.pdf (acedido a 18 de Março 2018)

[21] História secreta da Segunda Guerra Mundial (2018).Revista National Geographic – Parte 1 editora-RBA Portugal

[22] História secreta da Segunda Guerra Mundial (2018).Revista National Geographic – Parte 2 editora-RBA Portugal

[23] https://www.cia.gov/index.html (Consultado a 12 de Março)

[24] Página 15 e 16 de Silva, S. (2014). A Ciberespionagem no contexto português (Dissertação de Mestrado). Academia Militar, Lisboa.

[25]https://pt.wikipedia.org/wiki/Tratado_de_Segurança%C3%A7a_UK-USA [Consultado em 12 de Março 2018]

[26]https://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer [consultado a 12 de Março 2018]

[27]Mañas, A. P. (2017). ECHELON y la vigilancia masiva: entre la seguridad y la protección de la privacidad. Disponivel em

http://uajournals.com/ojs/index.php/cisdejournal/article/view/200 [consultado a 12 de Março de 2018]

[28] https://observador.pt/seccao/mundo/edward-snowden/ [consultado a 12 de Março de 2018]

[29] MOREIRA, João M. D. – O Impacto do Ciberespaço como Nova Dimensão nos Conflitos - Boletim Ensino | Investigação nº 13, Novembro 2012, Capítulo 2, p. 27-50. Disponível na Internet: http://www.iesm.pt/cisdi/boletim/Artigos/Artigo_2.pdf. [consultado 18 de Março de 2018].

[30] IDN nº 12 - Estratégia da Informação e Segurança no Ciberespaço - Investigação conjunta IDN-CESEDEN – Instituto de Defesa Nacional – 2013. Disponível em: http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf [Consultado 18 de Março 2018].

[31]http://content.time.com/time/nation/article/0,8599,1098371,00.html [consultado a 18 de Março de 2018]

[32] http://thehill.com/policy/technology/304111-report-china-hacked-obama-mccain-campaigns [consultado a 18 de Março de 2018]

[33]https://www.noticiasaominuto.com/mundo/982746/dirigente-da-campanha-de-trump-contactou-com-espionagem-russa [consultado a 29 de Março 2018]

[34] https://ionline.sapo.pt/604500 [consultado a 18 de Março 2018]

[35]http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.Wry71ufOXIU [consultado a 18 de Março 2018]

[36] http://cyber.harvard.edu/cybersecurity/GhostNet [consultado a 18 de Março de 2018]

[37] https://muitocurioso.org/operacao-aurora-serie-de-ataques-ciberneticos/ [consultado a 18 de Março 2018]

[38] Documentário Stuxnet - Zero Days http://www.imdb.com/title/tt5446858/ (Acedido a 18 de Março 2018)

[39] https://www.wired.com/2012/05/flame/ [consultado a 18 de Março 2018]

[40] https://securelist.com/the-red-october-campaign/57647/ [consultado a 18 de Março 2018]

[41]https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/?utm_term=.6505706afdd9 [consultado a 18 de Março 2018]

[42] http://expresso.sapo.pt/internacional/2018-02-11-Jogos-Olimpicos-de-Inverno-alvo-de-ataque-informatico-mas-origem-nao-e-revelada [consultado a 18 de Março 2018]

[43] https://threatpost.com/lookout-dark-caracal-points-to-apt-actors-moving-to-mobile-targets/130304/ [consultado a 18 de Março de 2018]

[44]https://www.theguardian.com/artanddesign/shortcuts/2015/mar/08/dead-drops-what-to-do-if-you-see-a-usb-stick-sticking-out-of-a-wall [consultado a 18 de Março 2018]

[45] http://news.bbc.co.uk/2/hi/europe/4639758.stm [consultado a 18 de Março 2018]

[46] https://www.scmagazine.com/cyberespionage-may-be-next-top-threat-to-businesses-this-year/article/644720/ [consultado a 18 de Março 2018]

[47] ISTR-Internet Security Threat Report Volume 22. Disponível em: https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf [Acedido em 28 de Março de 2018]

[48]https://www.forbes.com/sites/forbesleadershipforum/2013/05/13/your-business-is-never-too-small-for-a-cyber-attack-heres-how-to-protect-yourself/#af125aa54f65 [consultado a 21 de Março de 2018]

[49] Relatório ENISA- disponível em https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017 [consultado a 21 de Março 2018]

[50]https://www.enisa.europa.eu/topics/csirts-in-europe/capacity-building/european-initiatives/cert-eu [Consultado a 21 de Março de 2018]

Bibliografia

Frias, Óscar Luís Soeiro. (2013). Cyber intelligence a obtenção de informações a partir de fontes abertas no ciberespaço (Dissertação de Mestrado). Academia Militar, Lisboa.

Silva, S. (2014). A Ciberespionagem no contexto português (Dissertação de Mestrado). Academia Militar, Lisboa.

Esteves, Luís F. M. (2015) As vulnerabilidades do SEE- A cyber segurança (Dissertação de Mestrado)- Faculdade Engenharia Universidade do Porto

Magalhães, Joana B. N. P. (2016) wikileaks enquanto ator transnacional: que desafios para o estado? (Dissertação de Mestrado) Escola de Economia e Gestão- Universidade do Minho

Santos, Daniela G. G. (2014) A cibersegurança em Portugal: A ação política nacional em matéria de cibersegurança – (Dissertação de Mestrado) – Departamento de Ciência Política e Políticas Públicas -ISCTE IUL- Instituto Universitário de Lisboa

Mangiameli, A. C. (2016) THEORY OF LAW AND COMPUTER CRIMES- TEORIA DO DIREITO E CRIMES INFORMÁTICOS. Revista Duc In Altum Cadernos de Direito, vol. 8, n.º 16 , **17-41**

Teoh, C. S. e Mahmood A. R. (2017) National Cyber Security Strategies for Digital Economy. Faculty of Science & Information Technology Universiti Teknologi Petronas Malaysia

Goodman, Will (2010). Cyber Deterrence Tougher in Theory than in Practice? Strategic Studies Quarterly, **102-135**

Rid, Thomas (2012) Cyber War Will Not Take Place - King's College London, UK. The Journal of Strategic Studies Vol. 35, No. 1, **5–32**

Feldman, Jonah e Chow Ming (2017) The Internet's Security Dilemma: Why Cyber-Weapons Beget Instability- Disponivel em: http://www.cs.tufts.edu/comp/116/archive/fall2017/jfeldman.pdf

Webgrafia

https://www.theguardian.com/world/2006/jan/23/russia.politics

https://www.telegraph.co.uk/news/politics/2435859/Military-secrets-missing-on-Ministry-of-Defence-computer-files.html?DCMP=EMC-new_19072008

https://pt.wikipedia.org/wiki/USB_dead_drop

http://www.dailymail.co.uk/sciencetech/article-1326177/Dead-Drops-Bizarre-new-artwork-embeds-USB-sticks-buildings.html

https://pt.linkedin.com/pulse/li%C3%A7%C3%B5es-da-ciber-espionagem-para-seguran%C3%A7a-das-carlos-rodrigues

https://www.publico.pt/2017/04/10/tecnologia/noticia/ferramentas-de-ciberespionagem-da-cia-1768324

http://www.itchannel.pt/news/seguranca/equation-group-o-rei-da-ciber-espionagem

http://www.cio.pt/2017/03/23/deve-preocupar-se-com-a-ciber-espionagem/

https://sol.sapo.pt/artigo/50524/identificado-novo-tipo-de-malware-especializado-em-ciber-espionagem-

https://sol.sapo.pt/artigo/116189/eua-gastam-milhoes-a-protegerem-se-da-ciber-espionagem-chinesa

http://www.consilium.europa.eu/pt/press/press-releases/2017/12/20/cybersecurity-eu-institutions-strengthen-cooperation-to-counter-cyber-attacks/

http://www.consilium.europa.eu/pt/policies/cyber-security/

http://www.consilium.europa.eu/pt/press/press-releases/2017/11/20/eu-to-beef-up-cybersecurity/

https://www.cncs.gov.pt/transposicao-da-diretiva-nissri/

https://www.itworldcanada.com/article/398785-2/398785

https://www.whitehouse.gov/presidential-actions/president-donald-j-trump-proclaims-october-2017-national-cybersecurity-awareness-month/

https://www.acsc.gov.au/publications.html