

Information and security in cyberspace: The influence of globalization on the intensification of risks and threats in the last decade

Informação e Segurança no Ciberespaço: A influência da globalização na intensificação de riscos e ameaças na última década

Bruno Garcia³²

Centro de Administração e Políticas Públicas, Instituto de Ciências Sociais e Políticas,
Universidade de Lisboa, Portugal

RESUMO:

Este artigo fornece uma breve história da segurança de informação, com ênfase nas ameaças à segurança cibernética e como estas são influenciadas pela globalização. É realizada uma análise comparativa de três fontes diferentes para captar alguns padrões sobre esta relação: 1) relatórios da ENISA sobre ameaças cibernéticas, 2) relatório global de riscos, sobre ameaças globais e 3) relatório DHL-*Global Connectedness* para indicadores de globalização. Para evitar dispersão, a análise é circunscrita aproximadamente à última década. Este relatório aponta para uma intensificação das ameaças cibernéticas nos últimos anos, enquanto os indicadores de globalização sugerem um abrandamento nas interligações globais. São recomendadas para investigação adicional algumas hipóteses para explicar estes padrões.

Palavras-chave: Cibersegurança; Globalização; Segurança de Informação; Ameaças Globais

ABSTRACT:

This article provides a brief history of information security, with emphasis on cybersecurity threats and how these are influenced by globalization. A comparative analysis of three different sources is carried out to capture some patterns on this relationship: 1) ENISA reports on cyberthreats, 2) The Global Risks Report, on global threats and the 3) DHL-Global Connectedness report for globalization indicators. To avoid dispersion the scope of analysis is approximately the last decade. This comparative analysis points to an intensification of cyberthreats in the last few years while globalization indicators hint at a slowing down on global connections. Some hypotheses to explain these patterns are suggested for further research.

Keywords: Cybersecurity; Globalization; Information Security; Global threats

1. Introdução

A informação constitui um meio de eliminar incerteza (Gleick, 2011). Pelo menos desde que o Homem se organiza coletivamente que a informação se reveste de importância fulcral na

³² E-mail: garcia.bruno.c@gmail.com

ORCID: <http://orcid.org/0000-0003-1502-7567>

sua sobrevivência. Desde a pré-história, saber onde caçar, saber onde recolher alimentos, saber o que cultivar e em que momento, conferia uma vantagem competitiva avassaladora a algumas tribos e fazia a diferença entre sobreviver e perecer. Manter a informação segura, no sentido de a proteger contra divulgação ou modificação indevida, constitui, portanto, uma preocupação latente da humanidade desde tempos imemoriais. Todas as grandes civilizações ao longo da história constituíram redes de segurança de informação – passando pelo antigo Império Romano, com os *Frumentarii* (Gibbon, 1985), e o Império Chinês com os *Jinyiwei* (Miller, 2009), até às cortes europeias do Renascimento.

Este legado histórico e perene pode levar à tentação de afirmar que a segurança de informação não constitui uma realidade original – sempre existiu. Contudo, a globalização em geral e o ritmo acelerado do desenvolvimento tecnológico em particular, conferem à segurança de informação uma natureza diferente daquela a que tradicionalmente nos habituámos. As diferenças de escala importam, alterando muitas vezes a natureza intrínseca dos fenómenos, e o mundo interdependente, interconectado e globalizado em que vivemos alteraram profundamente o domínio da segurança (Nunes, 2016).

Foi a revolução industrial que começou a integrar diferentes regiões mundiais numa economia global. A globalização não constitui um desenvolvimento moderno, mas os avanços tecnológicos em transportes e comunicações, e particularmente em sistemas de informação, aprofundaram significativamente as ligações entre países, a complexidade das relações internacionais e a sua abrangência (Trade & Globalization, 2006). Também aqui as diferenças de escala contam e a globalização é hoje um fenómeno de natureza diferente da aceção tradicional.

Note-se que as reflexões sobre a globalização surgem quase sempre a par com o desenvolvimento tecnológico. Torna-se, portanto, fundamental perceber de que modo as ameaças existentes nesta arena tecnológica influenciam ou são influenciadas pela globalização. Uma perspetiva fundamentada sobre a forma como os padrões de inter-relação entre a cibersegurança e os indicadores de globalização se modificam ao longo do tempo é essencial para a tomada de decisões em políticas públicas neste domínio. A título de exemplo, os decisores políticos influenciam os fluxos de investimento estrangeiro através de políticas fiscais. Podem também incentivar, de forma mais ou menos ostensiva, a formação de profissionais tecnicamente preparados para lidar com as ameaças cibernéticas. A nível macro, os decisores políticos determinam os padrões de cooperação internacional para o combate ao cibercrime. O propósito deste artigo é precisamente delinear alguns padrões sobre a forma como a globalização e as ameaças em cibersegurança se inter-relacionam.

Sublinhe-se que não é pretensão deste trabalho estabelecer uma relação de causa efeito entre o aumento das ameaças de cibersegurança e a globalização, ou compreender em que medida a globalização potenciou o crescimento da rede eletrónica, ou a rede potenciou a globalização. É provável que a relação de causalidade seja bidirecional. A existência de fatores intermediários a mediar esta relação revestem-na de uma complexidade que não se pretende aqui explorar.

Para atingir o propósito definido, a próxima secção será dedicada a esboçar uma história recente da segurança de informação até à atualidade e a secção seguinte é dedicada a um caso de estudo específico – o impacto do malware NotPetya na Maersk e nas cadeias de fornecimento globais. Estas duas secções permitirão demarcar a globalização atual e o domínio da segurança de informação em particular como fenómenos essencialmente novos, vincando o caráter global das redes de informação e das ameaças que lhe subjazem.

Na secção subsequente será efetuada uma análise comparativa entre relatórios de cibersegurança emitidos pela European Union Agency for Cybersecurity (ENISA), os relatórios designados por The Global Risks Report do World Economic Forum e por fim, como barómetro da globalização, o DHL – Global Connectedness report. Para não sobrecarregar o artigo, a análise será circunscrita aos últimos dez anos. Por fim, procurar-se-á estabelecer alguns padrões gerais na relação entre a globalização e as ameaças de cibersegurança.

2. Segurança de informação: um esboço histórico

O quadro histórico mais recente que levou à aceção moderna de segurança de informação é seguidamente esboçado em traços muito gerais.

Na segunda guerra mundial, o sucesso dos primeiros computadores usados para decodificar comunicações alemãs tornou evidente o potencial destas máquinas para o armazenamento de informação e resolução de problemas complexos. Logo após a guerra, alguns governos investiram no desenvolvimento de tecnologia computacional – surgem os primeiros mainframes: grandes computadores dedicados a processos críticos ou a armazenar grandes conjuntos de dados. Nessa fase, a segurança destes ativos era de natureza física: a preocupação era manter protegidos os locais onde estavam alojados estes grandes computadores. Era também vantajoso transportar informação entre mainframes, porém fazê-lo era oneroso e ineficiente. Em simultâneo, o clima de guerra fria vincava a necessidade de redundância entre sistemas críticos. Estas dificuldades apenas seriam ultrapassadas se de

algum modo estes mainframes comunicassem entre si de forma automática. Na segunda metade da década de cinquenta do século XX, o departamento de defesa norte americano criou a Advanced Research Project Agency (ARPA) especificamente para resolver este problema. Em finais dos anos sessenta tinha-se tornado óbvio que este grupo, em concertação com outros grupos provenientes de meios académicos, científicos e corporativos tinham chegado a uma solução – tinha nascido a ARPANET: dois computadores em diferentes universidades californianas tinham estabelecido comunicação entre si. Ao longo dos anos seguintes estas ligações aumentaram, tendo-se adicionado nós à rede. Neste momento surgiram relatórios sobre as vulnerabilidades desta rede; começou a evidenciar-se que a segurança destes ativos transcendia a defesa física – surgem os primeiros protocolos de segurança, e mecanismos incipientes de segurança lógica (Yost, 2007). No início dos anos 70 surgiu também um programa experimental, desenhado para ser transportado entre sistemas operativos, entretanto melhorado para criar uma cópia de si próprio. Este programa, designado por CREEPER pelo seu criador, foi reconhecido como o primeiro vírus informático. Note-se que este programa não teve um efeito malicioso, despoletando apenas uma mensagem ao utilizador – mas o potencial de disrupção deste tipo de programa era evidente (DeNardis, L, 2007).

No final dos anos setenta, empresas como a Microsoft (na conceção de software), IBM, (sobretudo na produção de hardware) e a Apple, (no desenvolvimento de software e hardware), criaram as condições que permitiram levar um computador à casa de cada pessoa a preço razoável – surge o computador pessoal. Dá-se a descentralização da informação eletrónica: os grandes mainframes continuam a ser os ativos críticos, mas parte da informação está também diretamente disponível em cada dispositivo local, dando lugar à arquitetura que ficou conhecida como cliente-servidor.

O princípio elementar destas redes de comunicação informáticas era de que as mensagens podem ser fragmentadas, enviadas em rede numa série de transmissões e depois reagregadas no destino de forma rápida e eficiente. Para que isso fosse possível era aplicado um protocolo, ou conjunto de regras que permitem que os computadores funcionem em conjunto. Redes diferentes tinham protocolos diferentes, o que impossibilitava a comunicação entres estas. Este desafio foi também ultrapassado pelo ARPA (entretanto renomeado para DARPA, Defense Advanced Research Project Agency) cujos cientistas desenvolveram o protocolo TCP/IP que tornou possível a comunicação entre praticamente qualquer rede informática, independentemente do hardware, do software ou da linguagem usada. Com a implementação deste protocolo em 1983 consolida-se a internet, ou rede das redes

interconectadas. Durante algum tempo o projeto de criação de TCP/IP envolveu a implementação de mecanismos de encriptação, ou a prática de codificar mensagens de forma a que apenas o destinatário pretendido consiga descodificar, através de uma chave matemática. Mas este processo era oneroso, exigindo mais capacidade computacional e hardware específico. Nesta altura também não era claro como distribuir as chaves de encriptação de forma segura, um problema que ainda hoje complica os sistemas de encriptação. Perante estas barreiras intransponíveis o foco dos cientistas envolvidos continuou a ser o desafio técnico de movimentar informação rápida e fiavelmente. A perspetiva em relação à segurança era de que os riscos centrais da internet tinham a ver com ameaças militares, ou invasores externos à rede, mas poucos previram que os próprios utilizadores da rede a poderiam usar para atacar outros utilizadores, ainda que tivessem havido alguns alertas. Surgem pouco depois os primeiros ataques informáticos na aceção contemporânea do termo, tipicamente designados como hacking – ataques desencadeados remotamente, recorrendo à rede informática para, de forma intrusiva, obter informação ou de outro modo corromper um sistema hoje (DeNardis, L, 2007). Um dos casos mais célebres nos anos oitenta foi o ataque First National Bank of Chicago que terá levado ao roubo de setenta milhões de dólares.

Na sua conceção, a internet revela-se essencialmente rápida, eficaz, livre de atritos, mas também permeável e vulnerável. Estes elementos são essenciais para apreender o quadro em que se desenvolve a segurança de informação e os seus desafios.

No final dos anos 80, dá-se outra grande mudança: a internet abre-se ao público generalizado com a criação da World Wide Web. Dá-se uma quebra nos termos da interação entre partes que pode passar despercebida: com esta mudança altera-se a relação de confiança – dá-se um tipo de comunicação em que os intervenientes não conhecem necessariamente a entidade que está do outro lado. Passam a estar disponíveis na internet dados pessoais. As redes de crime organizado estão atentas e começam a procurar formas de explorar esta informação. Entretanto durante a década de noventa surge o comércio online, que rapidamente assume proporções impressionantes, gerando empresas e modelos de negócio inteiramente orientados às transações eletrónicas. A rede explode, desmultiplicando-se continuamente até aos dias de hoje (DeNardis, L, 2007).

Com o aumento do perímetro de segurança em rede as ameaças informáticas tradicionais dão um salto em sofisticação e ao mesmo tempo emerge toda uma gama de novos conceitos. Somos confrontados com um novo jargão: o malware – software malicioso para corromper um sistema, o adware – software instalado para desencadear publicidade online direcionada mas não necessariamente solicitada, o spyware – software específico para vigiar o

nosso comportamento online, o ransomware – o software que pode bloquear acesso a informação (por intermédio de algum mecanismo de encriptação que constitui também uma disciplina em evolução crescente) e que poderá ser desbloqueada em troca de um resgate, tipicamente pago em criptomoeda; o Phishing, técnica de engenharia social, que na prática constitui um mecanismo dissimulado de levar as vítimas a ter um comportamento online que normalmente não teriam – seja a cedência de dados pessoais, ou a cedência de credenciais de acesso a sistemas com informação sensível (Kim, D., & Solomon, M. G., 2016). Estes são apenas alguns exemplos dos termos atualmente em voga.

A disseminação desta tecnologia de comunicação em rede tem na sua base a propagação da infraestrutura física que a suporta. Tendemos a pensar na internet com um organismo suspenso no éter, mas é surpreendente verificar que este organismo tem na verdade um corpo: centenas de milhares de quilómetros de cabos, a percorrer estradas e linhas ferroviárias, torres de comunicações, satélites e grandes edifícios, designados por network exchanges, que são na prática grandes pontos de contacto da rede (Blum, 2012). O carácter transnacional destas estruturas físicas é também um dos fatores que caracteriza a internet como componente do mundo globalizado.

Para dar resposta ao aumento combinado, do perímetro de segurança, da complexidade dos sistemas e da sua abrangência, surgem regulamentos estruturados para proteção de dados – sendo neste âmbito o exemplo mais notório e atual o regulamento geral de proteção de dados. A disciplina de Segurança de Informação torna-se um domínio estruturado em diversas camadas: camada de proteção das pessoas, camada de proteção de hardware, de software, de dados, de processos e da rede. As distinções são por vezes vagas, mas é comum separar a cibersegurança da segurança de informação de forma mais lata, pelas camadas de segurança sobre a sua esfera de ação – a cibersegurança abrange essencialmente a segurança das camadas de software, dados e redes e, parcialmente, de hardware (Kim, D., & Solomon, M. G., 2016).

Como que para dar corpo às ameaças e aos conceitos de segurança de informação aqui enunciados e vincar a sua relação com o mundo globalizado analisemos brevemente o incidente de ransomware (o já mencionado resgate fraudulento a sistemas informáticos) que atingiu a Maersk em 2017.

3. A globalização das ameaças no ciberespaço: o caso Maersk

A Maersk é uma empresa colossal, com oito unidades de negócio, que incluem a gestão de aproximadamente oitenta portos, logística, construção de navios e exploração petrolífera. Com 574 escritórios a operar em cerca de 130 países a Maersk é um símbolo, por excelência, da corporação global. Em junho de 2017, um grupo de funcionários desta empresa nos escritórios de Copenhaga detetou um comportamento inusitado nos seus computadores - nos ecrãs apareciam mensagens que anunciavam: “Sistema de ficheiros em C: em reparação”, com um aviso para não desligar o computador. Noutros lia-se: “Oops, os seus ficheiros importantes foram encriptados” (Greenberg, 2019).

O contexto deste ataque é iminentemente geopolítico. Mais precisamente, a sua origem remete para o conflito entre a Rússia e a Ucrânia nos cinco anos anteriores ao ataque. Este conflito, iniciado por uma agressão da Rússia à Ucrânia, especificamente a tomada da península da Crimeia, terá desencadeado a maior crise de segurança na Europa desde a guerra fria. Vários estados intervieram para sancionar a Rússia, mas pouco foi conseguido no sentido de restaurar a integridade territorial na Ucrânia (Stanovaya, 2019). Em geopolítica, tal como em história, não existem causas únicas. Este conflito é complexo e escrutinar a sua natureza não caberá neste artigo. Será enfatizada apenas uma causa próxima: a Ucrânia era um elemento central de poder da ex-união soviética, tendo sido a segunda mais populosa e poderosa das quinze repúblicas soviéticas, sendo também um território encarado como o “celeiro” da união pelo seu peso na produção agrícola; detinha também muita indústria na área da defesa e militar, incluindo a frota do mar negro e algum arsenal nuclear. Após a queda da união soviética a Ucrânia procurou uma aproximação com o ocidente, designadamente a união europeia e a NATO; o que contraria as crescentes pretensões de hegemonia na região por parte da liderança Russa. Ao tomar a Crimeia a Rússia consolida o controlo do mar negro. Com uma presença militar neste espaço a Rússia poderá projetar influência para a região mediterrânica, para o médio oriente e para o norte de África. Ao mesmo tempo estreitam-se alianças energéticas e militares com a Turquia, a outra grande potência do mar negro (Stanovaya, 2019; Ramírez & Telman, 2016).

Em paralelo, um grupo de hackers ligados ao Kremlin, conhecido como Sandworm, tinha encetado um conjunto de ataques bem-sucedidos a outros países, incluindo os EUA. Este grupo tinha-se tornado uma das facetas mais proeminentes do potencial de ciberataque da Rússia. Com o prolongamento do conflito entre a Ucrânia e a Rússia, a Ucrânia tinha-se

tornado na prática um laboratório de teste para as capacidades Russas na arena cyber (Greenberg, 2019).

Na primavera de 2017 este grupo tinha conseguido penetrar num sistema alojado nos servidores da Linkos Group. Esta pequena empresa ucraniana alojava os servidores de atualizações – com correções de erros, remediações de segurança e novas funcionalidades – de um software de contabilidade designado por M.E.Doc. Este era o software mais comumente usado para a submissão de informação fiscal, estando presente na maioria das empresas na Ucrânia. Não se pretende aqui anatomizar este ataque com detalhes técnicos vincando-se apenas que na prática os atacantes tinham conseguido uma porta de entrada a todos os computadores que tinham instalado o M.E.Doc. Aproveitando esta porta de entrada, em junho desencadearam a campanha de ransomware através de um pedaço de código malicioso designado por NotPetya. O ataque foi avassalador, tendo atingido diversas entidades e empresas na Ucrânia, designadamente alguns dos maiores bancos, dois aeroportos, hospitais, companhias energéticas e sistemas diversos de pagamento. É pertinente assinalar que inúmeras entidades pagaram o resgate – sem efeito. Nesta altura a equipa de informática do escritório da Maersk na cidade ucraniana de Odessa tinha instalado o M.E.Doc num único computador – foi o suficiente para comprometer inexoravelmente grande parte da interligada infraestrutura informática da companhia.

O impacto foi devastador. O software dos navios da Maersk não foi afetado, mas o software dos terminais portuários - desenhado para atualizações automáticas de dados sobre mercadorias transportadas e esperadas nos portos - deixou de funcionar, inviabilizando a complexa gestão do carregamento e descarregamento dos contentores. Em dezassete dos quase oitenta portos geridos pela Maersk geraram-se filas de camiões à espera de instruções. Vejamos apenas alguns exemplos da abrangência deste impacto: a Merck, grande empresa farmacêutica, ficou temporariamente incapacitada de produzir novos fármacos, a TNT Express não conseguia expedir ou receber encomendas, a construtora Saint-Gobain ficou sem matérias primas. Todas estas empresas incorreram em perdas financeiras que ascendem a milhões de euros. Inúmeras empresas que dependem da entrega imediata e atempada de produtos foram afetadas.

A recuperação deste desastre foi pesada e morosa, envolvendo a nível técnico a recuperação de cópias de segurança (backups) de toda a informação eletrónica contida nos servidores da Maersk antes do ataque. Um aspeto técnico em particular ilustra a dimensão do problema: existe uma camada essencial na infraestrutura informática organizacional correspondente a um tipo de servidor denominado por domain controller. Estes servidores

fornecem um mapa detalhado da rede informática de uma organização e incorporam as regras elementares que determinam a que sistemas os utilizadores podem aceder. A Maersk tinha cerca de 150 domain controllers programados para sincronizar informação, precisamente numa lógica de redundância. Mas esta configuração não previa um cenário em que todos estes servidores fossem corrompidos ao mesmo tempo. Sem estes servidores, dificilmente seria possível recuperar outros componentes da rede. Os técnicos informáticos conseguiram detetar um domain controller não corrompido – devido a uma fortuita quebra de energia - nas instalações da Maersk no Ghana e executar a laboriosa tarefa de copiar a informação neste servidor para outros centros de dados. A companhia demorou duas semanas a estabilizar a sua rede o suficiente para voltar a ligar postos de trabalho – em computadores “limpos” - e meses a estabilizar as suas operações. O desastre expôs falhas nas políticas de segurança da empresa, salientando-se o recurso a software datado, a não remediação de vulnerabilidades em diversos sistemas; a não atualização de sistemas operativos e a falha em recorrer a mecanismos de acesso de múltipla autenticação em sistemas críticos. Os custos incorridos pela Maersk, onde se inclui o pagamento de compensações a clientes, são difíceis de medir.

A intenção do ataque não é inteiramente clara. Greenberg (2019) especula que esta operação permitiu varrer da rede vestígios de espionagem ou planos de sabotagem futura e em simultâneo deixar um aviso: qualquer empresa a manter operações em território ucraniano pode incorrer em custos avultados. É possível também que o seu impacto global não fosse antecipado pelos próprios atacantes – alastrou-se até a algumas empresas russas, destacando-se a empresa energética estatal, a Rosneft.

Independentemente da sua intenção, este caso desvenda uma realidade incontornável: é hoje possível uma nação ou grupo mobilizar uma arma numa arena onde não existem fronteiras, onde a distância verdadeiramente não importa. Um ataque a uma pequena empresa na Ucrânia atingiu a Maersk e por esta via grande parte do mundo comercial. Subjacente a este ataque sobressai uma lógica de causalidade muito específica do domínio do ciberespaço.

Na secção seguinte, serão comparados alguns relatórios de cibersegurança, relatórios de ameaças globais e indicadores de globalização com vista a estabelecer alguns padrões entre a globalização e as ameaças de cibersegurança na secção final.

Análise dos relatórios de cibersegurança, relatórios de ameaças globais e indicadores de globalização

Nesta secção serão comparadas três fontes de informação, no sentido de identificar alguns padrões na relação entre as ameaças de cibersegurança e a globalização.

A primeira fonte de informação são os ENISA Threat Landscape reports respeitantes às ameaças de Cibersegurança no espaço Europeu (ENISA, 2019)³³. Esta fonte é selecionada essencialmente por constituir uma das bases para elaborar políticas públicas na área de cibersegurança entre os estados membros da União Europeia. A informação coligida para estes relatórios provém de três fontes: a) o MISP, uma plataforma aberta para a partilha de informação sobre malware financiada pela União Europeia, b) o CERT-EU, Computer Emergency Response Team para as instituições da União Europeia e c) o portal da empresa Cyjax, empresa especializada em serviços de inteligência em ameaças digitais.

Nas sete edições publicadas deste relatório é mostrada uma lista ordenada das 15 principais ameaças de cibersegurança para o período em análise. O gráfico 1, mostra as posições relativas das ameaças de cibersegurança desde 2012 até 2018, tendo por referência o ranking do último ano.

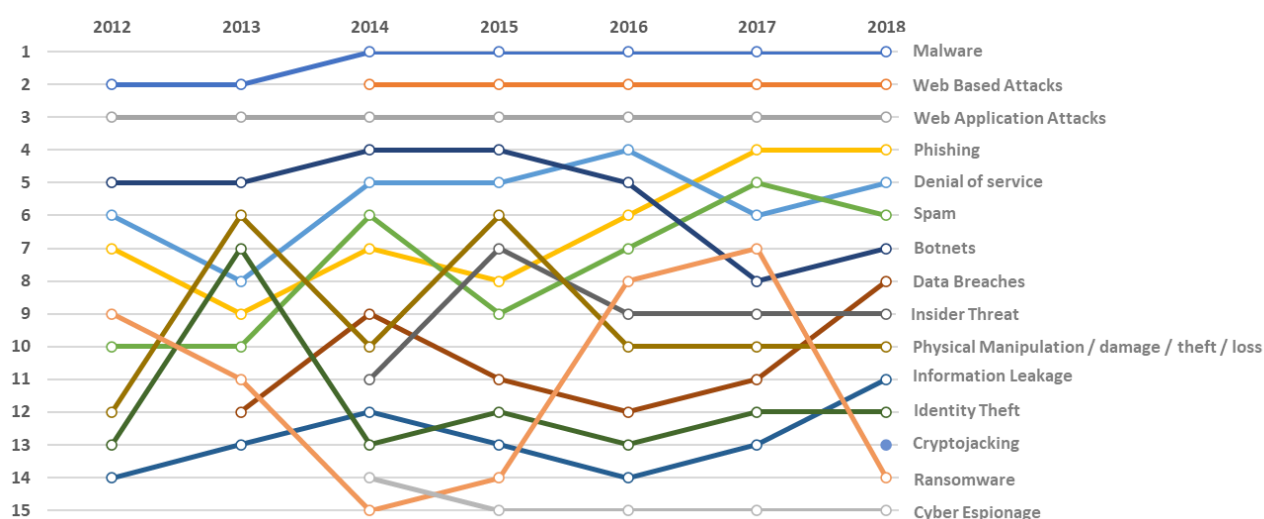


Gráfico 1: Top 15 das ameaças de cibersegurança desde 2012 até 2018, tendo por referência o ranking de 2018, a partir dos *ENISA Threat Landscape reports* de cada ano.

Em seguida descreve-se sumariamente cada ameaça, pela ordem apresentada no ranking de 2018. Pelo seu carácter generalizado no jargão da área de segurança de informação, optou-se por manter a designação anglófona original. 1) Malware é a designação dada a software malicioso – note-se que esta designação é explicitamente incluída apenas em 2014; nas edições anteriores esta categoria era mais específica, com a designação de Virus (que se

³³ A referência incluída em bibliografia corresponde ao relatório mais recente, para não sobrecarregar esta secção. Na prática, o mesmo endereço permitiu consultar todas as edições do relatório.

propagam parasitando outros ficheiros) e Worms (semelhantes aos vírus, mas potencialmente mais destrutivos por não precisarem de parasitar outros ficheiros); 2) Web based attacks, são ataques que usam sistemas e serviços da rede eletrónica como o meio ou arena principal para comprometer o alvo; 3) Web application attacks são as tentativas diretas ou indiretas de explorar uma vulnerabilidade em serviços ou aplicações na web; 4) Phishing, já mencionado em secção anterior, é um mecanismo de engenharia social por via eletrónica; 5) Denial of service (DoS) ou negação do serviço é uma ameaça de grande impacto, em que os atacantes procuram essencialmente negar o acesso ou interromper determinado sistema ou aplicação; 6) Spam, corresponde ao uso abusivo do email ou tecnologias de mensagens para inundar utilizadores com informação não solicitada; 7) Botnets, corresponde a uma rede de robots ou dispositivos interligados na web que podem ser usados em conjunto para negação de serviço (Distributed Denial of Service - DDoS), Spam ou roubo de informação; 8) Data breaches ou comprometimento de dados corresponde uma tentativa maliciosa de ataque bem sucedida, que levou ao comprometimento ou perda de informação; 9) Insider threat, ou ameaça interna, o que pode significar interna em relação a uma entidade, organização e empresa e que corresponde à ameaça representada pela possibilidade de indivíduos abusarem, de forma intencional ou não intencional, do acesso a ativos digitais; 10) Physical manipulation/damage/theft/loss, não sendo propriamente uma ameaça de cibersegurança, possibilita ainda assim o comprometimento de ativos digitais e podem levar a perdas de informação; 11) Information Leakage ou fuga de informação, pode abranger dados pessoais recolhidos por empresas a operar na Web, ou dados corporativos armazenados em infraestruturas de IT expostos de forma não desejada; 12) Identity theft ou apropriação de identidade corresponde a fraude decorrente do roubo de informação pessoal e proporcionada pela digitalização massiva de dados pessoais; 13) Cryptojacking, também conhecido como cryptomining refere-se a programas que usam abusivamente a capacidade de processamento de um determinado alvo, para processos de verificação e validação de transações de criptomoeda – processos muito exigentes computacionalmente; 14) Ransomware, ou resgate ilícito de sistemas digitais foi detalhado na secção anterior – o atacante assume controlo sobre ficheiros ou dispositivos e bloqueia o acesso ao seu responsável legítimo; para ceder controlo é tipicamente pedido um resgate em criptomoeda e por fim 15) a Cyberespionage, seja corporativa ou alavancada por nações-estado, categoria que tem ganho proeminência, e que corresponde a uma classe genérica de técnicas aplicadas para exercer influência geopolítica, ou roubar informação comercial e estatal ou ainda roubar propriedade intelectual , particularmente em domínios estratégicos.

Note-se que algumas das categorias listadas estão interligadas ou são muito dependentes entre si. A própria ENISA fez ajustes às categorias ao longo do tempo. A título de exemplo, a categoria de ransomware surgiu apenas em 2014, sendo que previamente existia uma categoria com designação de rogueware ou scareware. Para garantir continuidade comparativa, no gráfico optámos por considerar estas categorias equivalentes, daí que a linha de ransomware se estenda até 2012. A categoria de malware também surge em 2014, sendo que antes abrangia as designações mais específicas de Virus e Worm – também aqui optámos por considerar estas categorias equivalentes, o que explica a linha logo a partir de 2012. Por outro lado, a categoria de Web based attacks, terá substituído pelo menos uma categoria de especificidade um pouco diferente - drive-by exploits (correspondente a ocorrência de infeção de um sistema resultante da visita a sítio de internet malicioso) – neste caso optou-se por uma quebra de série, assumindo que a ameaça surge apenas em 2014 entre as 15 principais ameaças.

Feitas estas reservas, é possível retirar alguns padrões gerais. As categorias nas três primeiras posições são fundamentalmente as mesmas na última década: malware, Web based attacks e Web application attacks, o que é revelador do carácter abrangente destas categorias – constituem como que uma macro categoria em relação a outras. A categoria de ransomware revela o comportamento mais variável nestes rankings, o que estará relacionado com o carácter disruptivo desta ameaça nos anos em que ocorrem ataques bem-sucedidos (Wannacry e Not-Petya em 2017). As categorias relacionadas com Data Breaches e Identity Theft revelam algum alinhamento entre si, em posições diferentes do ranking, o que vinca a interdependência entre estas categorias – a perda de informação pessoal permitirá a apropriação de identidade. Importa destacar também a entrada em cena de novas categorias em 2014, como a insider threat, como categoria específica, e também a cyberespionage, coincidindo com o momento em que os primeiros grandes ataques promovidos por nações ganharam visibilidade mediática – nem uma nem outra categoria revelam indícios de virem a ser retirados da lista de ameaças mais proeminentes. Também visível no gráfico e apontado nas conclusões do último relatório, o email e o Phishing consolidaram-se como mecanismo principal ou vetor inicial de infeção (na quarta posição no último ano). Por fim, a necessidade de converter agilmente ativos em dinheiro introduziu no último ano analisado uma nova ameaça, o Cryptojacking, que na prática permite o aproveitamento de recursos computacionais para gerar criptomoeda, muitas vezes usada para encobrir pagamentos em atividades ilícitas, como o ransomware.

Uma das fontes para sondar ameaças mais abrangentes, são os Global Risk reports, promovidos pelo World Economic Forum (World Economic Forum, 2019³⁴), que incluem categorias de risco mais diretamente relacionadas com dinâmicas de globalização. Estes relatórios são elaborados anualmente com base em inquéritos a centenas de especialistas em diferentes domínios e as ameaças são ordenadas em função de impacto e probabilidade de ocorrência – sendo que o risco é normalmente medido como o produto entre impacto e probabilidade. Tendo por referência as últimas dez edições deste relatório propõe-se em seguida analisar o posicionamento que as ameaças tecnológicas relacionadas com a segurança de informação assumem entre as ameaças globais. Note-se que, desde 2012, estes relatórios contemplam três categorias associadas à segurança informática – a a) cibersegurança, b) fraude e roubo de dados e c) colapso de infraestrutura crítica de informação – existe outra categoria no domínio da tecnologia, designada por riscos decorrentes de avanços tecnológicos – demasiado genérica para ser incluída no grupo dos riscos de segurança de informação na aceção deste artigo. O Global Risks Report contempla outras 26 categorias de risco, em domínios como a Economia, a Geopolítica e o Ambiente.

O gráfico 2 apresenta precisamente o posicionamento das categorias diretamente relacionadas com riscos de segurança de informação na lista ordenada dos dez riscos principais, nas dimensões de impacto e probabilidade, ao longo da última década.

O primeiro dado a apontar a partir da observação do gráfico, é a de que em 2011 não se registaram ameaças de segurança de informação entre as dez ameaças globais principais. Nesta edição o relatório não contemplava as categorias de cibersegurança nem a categoria de fraude de dados, mas já incluía a categoria de colapso de infraestruturas de informação críticas e uma categoria entretanto descontinuada - segurança de Informação e dados online. É curioso notar que nesta edição de 2011 os riscos específicos de cibersegurança eram assinalados numa secção à parte, como riscos a monitorizar – essencialmente por falta de consenso entre os peritos no que respeita a níveis de confiança ou grande disparidade na aferição de impacto e probabilidade para estas categorias de risco. Apenas a partir de 2012, surgem as categorias específicas de cibersegurança e fraude de dados.

Analisando especificamente o eixo da probabilidade de ocorrência ao longo da última década, o risco de cibersegurança é destacado em termos de probabilidade de ocorrência a partir de 2012 – apenas em 2015 e 2016 não surge na lista dos 10 mais evidentes. Por outro lado, o risco de fraude ou roubo de dados surge na lista dos dez riscos principais em termos de

³⁴ Neste âmbito nem todos os relatórios estão disponíveis no mesmo sítio de internet, pelo que se incluem duas referências distintas na bibliografia. Na prática, foram consultados todos os relatórios desde 2011.

probabilidade de ocorrência a partir de 2015 e mantém-se na lista de riscos principais até à edição mais recente. Note-se que partir de 2017, há dois riscos associados à segurança de informação nas dez primeiras posições em termos de probabilidade.

Em termos de impacto, os riscos de segurança de informação surgem apenas pontualmente, em categorias diferentes, em 2014 e 2015, mas a partir de 2018 o risco de cibersegurança emerge entre os 10 principais e no ano seguinte surge também o risco de colapso de infraestrutura crítica de informação.

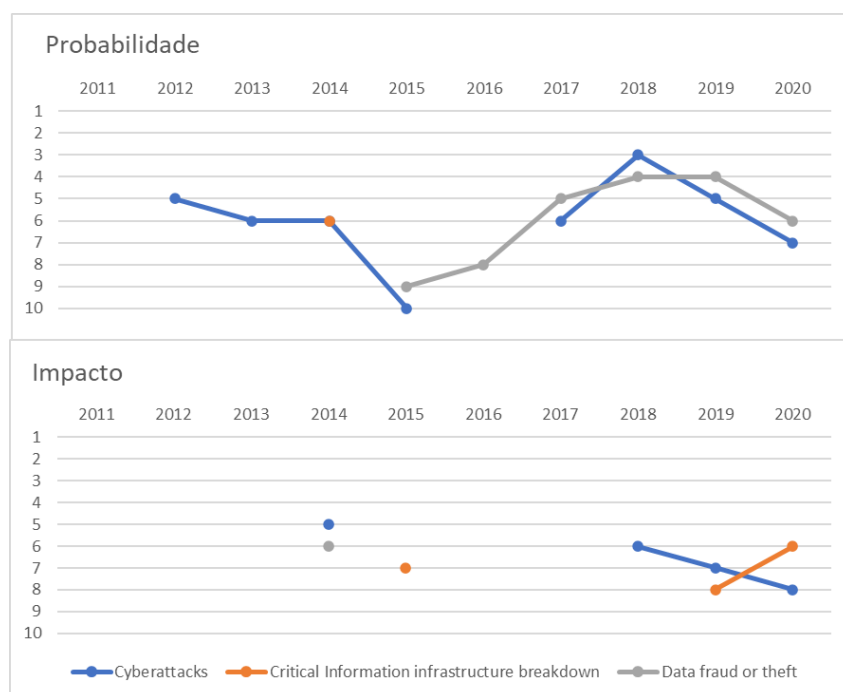


Gráfico 2. Posicionamento das categorias diretamente relacionadas com riscos de segurança de informação no ranking dos dez riscos principais, nas dimensões de impacto e probabilidade (2011-2020; Fonte: *World Economic Forum*)

Por fim, saliente-se um relatório que procura medir o grau das interligações globais, o DHL Global Connectedness Report (a seguir designado apenas por DHL-GCR) da autoria de Pankaj Ghemawat, Steven Altman e Phillip Bastian (DHL, 2019). Na prática estes autores produzem um índice de globalização a partir de quatro grandes dimensões: fluxos de capital, fluxos comerciais, fluxos de informação e fluxos migratórios. Segue-se uma amostra de alguns dos indicadores usados nestas dimensões, obtidos de entidades oficiais: fluxos de investimento direto estrangeiro entre países, número de turistas entre países, tráfego de internet entre países, número de estudantes universitários estrangeiros, número de residentes estrangeiros. Há neste relatório a preocupação de ponderar cada indicador com critérios

explícitos e recorrer a métricas relativas, em vez de absolutas. A abordagem metodológica do relatório está detalhada na secção VI do mesmo. Independentemente do rigor metodológico subjacente à elaboração do relatório, é importante vincar que medir uma realidade tão complexa como a globalização reveste-se de desafios difíceis de ultrapassar. Os autores reconhecem, por exemplo, a dificuldade em medir os fluxos de informação. Num sentido mais lato, a redução do conceito de globalização a um conjunto de indicadores gerais, levará a perder informação relevante para captar elementos fundamentais deste fenómeno. Não obstante, tendo presente que estes indicadores captam apenas parcialmente as dinâmicas de globalização é possível identificar alguns padrões de interesse para o propósito deste artigo.

Como forma de medir as dinâmicas comerciais, o relatório DHL-GCR apresenta um gráfico com a distância média percorrida por mercadorias a nível global, desde 2001. Após uma queda a seguir a 2001 até 2003, este indicador registou um aumento progressivo – mas é também notório que a partir de 2012 terá atingido um planalto, sem, contudo, apresentar indícios de queda subsequente.

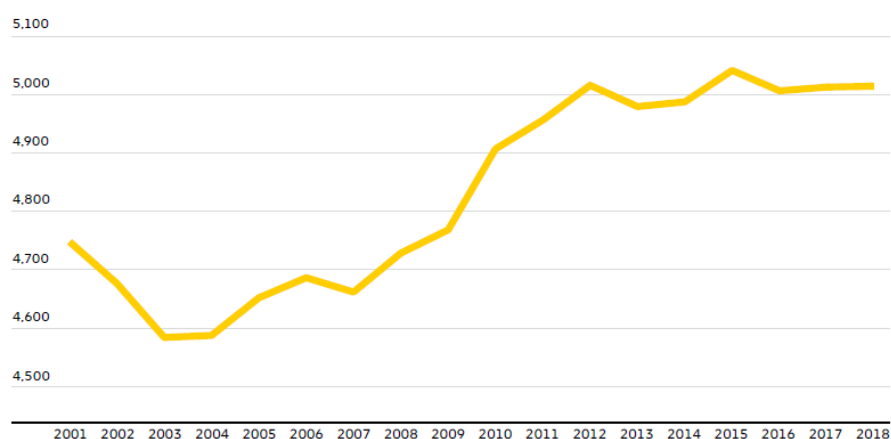


Gráfico 3: Distância média percorrida por mercadorias (em kms), 2001-2018 (Fontes de informação: IMF Direction of Trade Statistics (DOTS); UN Comtrade e CEPII GeoDist database)

Outro indicador interessante, mostrado no gráfico 4, tem a ver com fluxos de informação – designadamente a proporção de tráfego de internet internacional e a proporção de chamadas (a incluir VoIP) internacionais. No caso da internet regista-se um padrão de crescimento, quebrado entre 2010 e 2012, a acentuar-se depois até 2015, sendo que a partir desta fase o indicador estabiliza perto dos 20%. No que respeita as chamadas telefónicas, este

indicador regista um aumento continuado até 2014, momento em que desacelera e começa a estabilizar perto dos 7% em 2018.

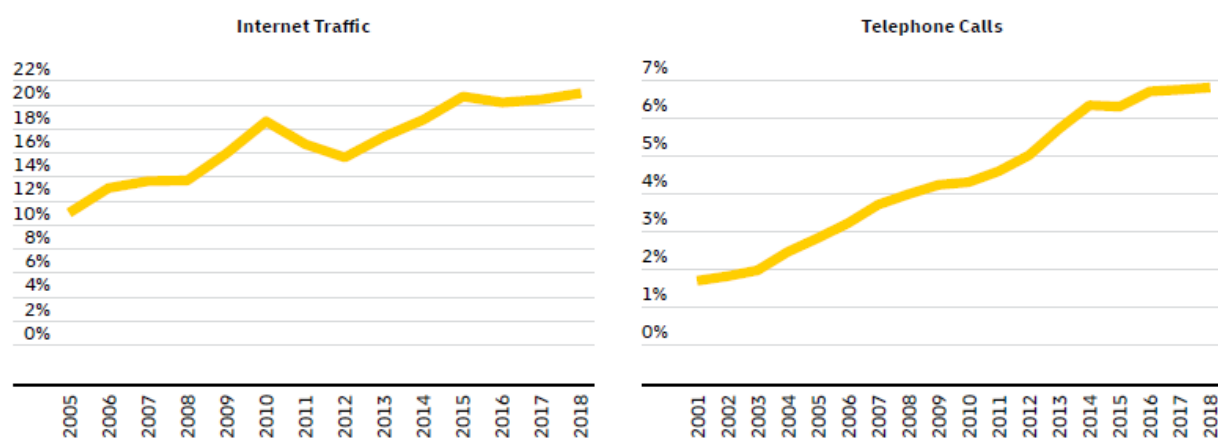


Gráfico 4: Tendências de Informação: Percentagem de tráfego de internet internacional (2005-2018) e Percentagem de tráfego em chamadas telefónicas (2001-2018)

O DHL-GCR inclui os resultados de um inquérito a 6035 gestores de empresas em três economias avançadas – Alemanha, Reino Unido e Estados Unidos) e três economias emergentes (Brasil, China e Índia) que permite vislumbrar uma terceira tendência que é interessante enfatizar. Esta tendência é representada no gráfico 5, que compara os valores efetivos de alguns dos indicadores de globalização, com as perceções dos respondentes em relação a estes mesmos indicadores. Observando o gráfico, torna-se imediatamente óbvio que estes gestores sobrestimam significativamente todas as medidas de interligação global. Este resultado indicia que as pessoas não estimam devidamente os limites da globalização e tendem a considerar que o mundo é mais interligado do que efetivamente é. Veja-se por exemplo o indicador analisado mais acima, sobre o tráfego de chamadas telefónicas – em média, os gestores inquiridos assumem que 35% do tráfego é internacional, mas o valor efetivo estimado para esta métrica ronda os 7%.

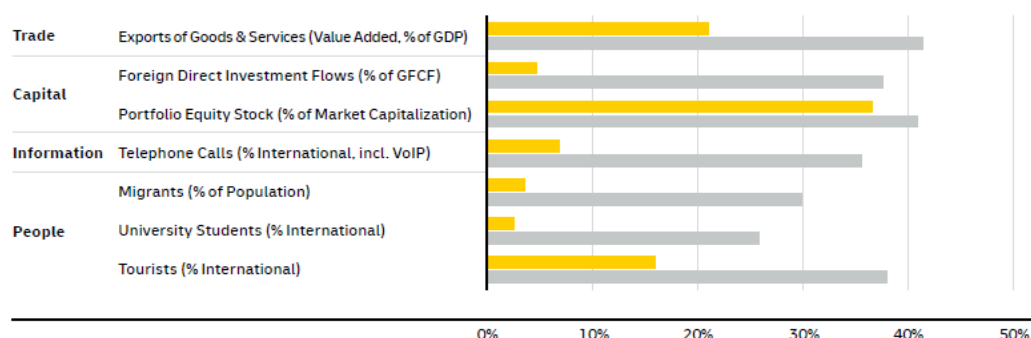


Gráfico 5: Medidas de globalização VS Percepções de gestores (linha amarela: Resultado efetivo estimado; linha cinzenta: valor percecionado por gestores de 6 países).

A partir da análise destes resultados, na secção seguinte serão propostos alguns padrões de influência entre a globalização e as ameaças em cibersegurança.

4. Análise dos padrões de influência entre a globalização e as ameaças em cibersegurança

Analisando os relatórios patentes na secção prévia, podemos destacar três grandes padrões, um em cada relatório: 1) No contexto específico das ameaças de segurança, há a registar a emancipação da categoria de cyberespionage nas dez principais ameaças, muito associada a grandes ataques promovidos por nações-estado e também o cryptojacking, que indicia uma necessidade crescente de monetizar ativos ilicitamente; 2) As ameaças de segurança de informação ganharam proeminência nos últimos anos no quadro de análise das ameaças globais – sendo que duas categorias de ameaça de segurança de informação surgem entre as 10 principais nos últimos anos, tanto em termos de impacto como de probabilidade e 3) Uma parte dos indicadores de interligação global, ainda que não evidenciem sinais de decréscimo, apresentam uma tendência de abrandamento nos últimos anos e são percecionados como mais intensos (pelo menos entre quadros administrativos) do que realmente são.

Nunca, como atualmente as questões de cibersegurança dominaram tanto os meios de comunicação social. Casos como o escândalo da consultora Cambridge Analytica, em que milhões de registos pessoais no Facebook foram usados sem consentimento para influenciar intenções de voto, exacerbam receios de manipulação e perda de privacidade (Cadwalladr & Graham-Harrison, 2018). Altos dirigentes governamentais mencionam frequentemente o ciberespaço como arena de oportunidades e ameaças. As grandes potências mundiais desenvolveram sofisticados dispositivos de recolha e análise de informação à escala global,

escudando-se na necessidade de garantir a sua segurança e defesa nacional (Nunes, 2016).

As ameaças do ciberespaço não são fáceis de definir e surgem muitas vezes como parte do menu das ameaças híbridas, ou seja, ameaças por adversários que recorrem simultaneamente a meios convencionais e não convencionais para prosseguir os seus objetivos de forma adaptativa. A lista de tecnologias exploradas no ciberespaço continua a aumentar: além dos servidores, computadores pessoais, e computadores portáteis, temos também de considerar os smartphones, os dispositivos de medição inteligentes (ex. contadores de consumo elétrico); pacemakers sem fios; sistemas eletrónicos de controlo industrial, etc. A gestão desta complexidade tem gerado apelos de governação da internet o que remete para o envolvimento do setor privado e da sociedade civil, nos seus respetivos papéis, na aplicação de princípios, normas e regras partilhadas, bem como procedimentos de tomada de decisão e programas que moldam a evolução e utilização da internet. Contudo, é notório que não há um estado, organização, ou instituição com capacidade para autonomamente governar a internet.

A governação da internet é incorporada nas inúmeras infraestruturas, dispositivos, fluxos de dados, e arquiteturas técnicas que – de forma discreta, por vezes invisível- subjazem e constroem a crescentemente articulada rede das redes (Bachman, 2012). Também por este prisma, a globalização fornece o quadro de fundo para a evolução da internet. É também desta perspetiva que as influências entre as ameaças no ciberespaço e os indicadores de globalização merecem atenção.

Por outro lado, os receios inerentes à globalização são também conhecidos – para os seus críticos a globalização não terá base filosófica e constitui apenas uma forma moderna de colonialismo económico e cultural que recorre a leis de propriedade intelectual para se impor em áreas fundamentais como a produção alimentar ou a saúde (Stiglitz, 2002). Porém as previsões de que a globalização iria ruir sobre o peso dos nacionalismos económicos tem-se verificado tão equivocada como as proclamações do mundo plano – baseado na noção de uma esfera competitiva crescentemente equilibrada entre países - que dominavam o discurso político há uma década (Ghemawat & Altman, 2019).

Biliões de pessoas usam tecnologias de informação e comunicação para conduzir os seus negócios, para interagir entre si e com governos. Uma elevada proporção destas pessoas iniciou-se neste domínio digital apenas recentemente. Se os decisores políticos assumirem uma relação inexorável entre as ameaças em cibersegurança e a intensidade da globalização, as soluções políticas serão diferentes daquelas que assumem a possibilidade de construir um ciberespaço mais seguro e de maior confiança. Estas soluções podem passar por desenvolver, a nível internacional, regras de comportamento no ciberespaço que possam reduzir ameaças,

aumentar a confiança e apoiar a melhoria da segurança no ecossistema cyber. Uma interpretação precisa das ameaças cibernéticas e da sua relação com outras ameaças globais, permitirá desenhar planos de recuperação de desastre mais resilientes.

5. Notas conclusivas

Emerge um elemento contraintuitivo da análise efetuada neste artigo: a intensificação das ameaças em cibersegurança surge na altura em que as dinâmicas de interligação global parecem estar a abrandar – tendência que eventualmente se tornará mais vincada no rescaldo do atual contexto de pandemia de Covid-19. Ainda que os receios de globalização e das ameaças de cibersegurança pareçam andar a par no debate público, a sua realidade prática parece desfasada.

Dar-se-á o caso de as ameaças de cibersegurança atenuarem as dinâmicas de interligação global? Ou será que a globalização está a estagnar exceto no domínio específico da inovação tecnológica? É provável, mas os dados neste relatório não fornecem dados suficientes para responder a estas hipóteses. Contudo, é evidente que os ciberataques constituem atualmente um fator de disrupção em si mesmo e já não são desencadeados apenas como mecanismo de suporte a ataques convencionais. A relação entre os padrões de globalização e as ameaças em cibersegurança e o consequente impacto em políticas públicas merecem investigação adicional.

Referências

- Bachmann, S. D. (2012). *Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats—mapping the new frontier of global risk and security management*. Amicus Curiae, 88.
- Blum, A. (2012). *Tubes: A Journey to the Center of the Internet*. New York: Ecco.
- Cadwalladr, C., & Graham-Harrison, E. (2018). The Cambridge analytica files. *The Guardian*, 21, 6-7.
- DeNardis, L. (2007) A History of internet security In de Leeuw, K. M. M., & Bergstra, J. (Eds.). *The history of information security: a comprehensive handbook*. (pp 595-621) Elsevier.
- DHL (2019). *DHL Global Connectedness Index*. Retirado a 5 de Abril de 2020, de <https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/g0-en-gci-2019-update-complete-study.pdf>

- ENISA (2019). *ENISA Threat Landscape Report*. Retirado a 30 de Março de 2020, de <https://www.weforum.org/reports/the-global-risks-report-2020>
- Ghemawat, P., & Altman, S. A. (2019). The State of Globalization in 2019, and What It Means for Strategists. *Harvard Business Review*.
- Gibbon, E. (1985). *The decline and fall of the Roman Empire: an abridged version*. Penguin Books.
- Gleick, J. (2011). *The information: A history, a theory, a flood*. New York, NY, US: Pantheon.
- Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.
- Joseph. E. Stiglitz. (2002). *Globalization and its discontents*. Penguin.
- Kim, D., & Solomon, M. G. (2016). *Fundamentals of information systems security*. Jones & Bartlett Learning.
- Miller, H. (2009). The Wanli Emperor, 1596–1606. In *State versus Gentry in Late Ming Dynasty China, 1572–1644* (pp. 75-94). Palgrave Macmillan, New York.
- Nunes, P.F..(2016). Ciberameaças e quadro legal dos conflitos no ciberespaço In Borges, J. V., & Rodrigues, T. F. (Eds). *Ameaças e Riscos transnacionais no novo Mundo Global*. (pp. 199-216). Porto: Fronteira do Caos.
- Ramírez, S. Telman, P. (2016). The Conflict in Ukraine: The First Serious Confrontation between Russia and the West in the Post-Cold War Age. *Foro internacional*, 56(2), 470-502. Retirado a 10 de abril de 2020, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0185-013X2016000200470&lng=es&tlng=en.
- Stanovaya, T. (2019, Dezembro). *What the West gets Wrong about Russias intentions in Ukraine*. Retirado a 12 de Abril de 2020, de <https://foreignpolicy.com/2019/12/06/what-the-west-gets-wrong-about-russias-intentions-in-ukraine/>
- Trade & Globalization (2006) *Chambers Dictionary of World History*. Chambers.
- World Economic Forum (2015). *The global Risks Report 2016* http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf
- World Economic Forum (2019). *The global Risks Report*. Retirado em <https://www.weforum.org/reports/the-global-risks-report-2020>
- Yost, R. (2007) A History of computer security standards In de Leeuw, K. M. M., & Bergstra, J. (Eds.). *The history of information security: a comprehensive handbook*. (pp 595-

621) Elsevier.