ESPIONAGEM CIBERNÉTICA EM TEMPOS DE COVID-19

Bruna Toso de Alcântara[1]

A dependência tecnológica da sociedade do século XXI não é algo novo, tão pouco o uso do ciberespaço como um novo meio de competição geopolítica. De acordo com Buchanan (2020, p. 3, tradução nossa) uma nova forma de estadismo surge com hackers governamentais jogando um "jogo interminável de espionagem e decepção, ataque e contra-ataque, desestabilização e retaliação". Essa nova tendência de estadismo não deixaria de cessar em tempos de pandemia.

O que torna essa nova forma de estadismo mais relevante nesses tempos de incerteza é a viabilidade do transbordamento das atividades digitais para o mundo físico envolvendo a perda de vidas humanas. Em outras palavras, a probabilidade dos efeitos do mundo digital se materializarem no mundo físico é alta quando os alvos de ataques cibernéticos se tornam infraestruturas críticas relacionadas a saúde. Sendo potencializados quando, em um movimento não precedente de presença online, grande parte da população conduz uma série de atividades sem os cuidados adequados de higiene cibernética ou sem pensamento crítico ante a busca por informações relacionadas ao novo vírus, que acabam alimentando campanhas de desinformação.

O uso de hackers patrocinados pelos Estados pode levar a reconfigurações ou reações no cenário internacional com consequências que podem perdurar mais tempo que o atual coronavírus. Dessa forma, o presente artigo busca esclarecer em particular como uma das atividades que compõe a nova forma de estadismo, a espionagem no ciberespaço, vem se desenvolvendo durante a pandemia e quais reações isso tem gerado no mundo físico.

Espionagem cibernética durante a pandemia

Desde o início da pandemia observou-se um aumento crescente de atividades maliciosas online. Segundo Izumi Nakamitsu (2020), alta representante das Nações Unidas (ONU) para desarmamento, houve um aumento de 600% em emails maliciosos durante a pandemia de COVID-19, além de relatórios no mundo todo apontando para ataques contra organizações de saúde e instalações de pesquisa médica. Esses atores maliciosos agem "tirando proveito de características humanas como curiosidade e preocupação com a pandemia de coronavírus" (NCSC; CISA, 2020, p.3, tradução nossa).

De fato, segundo Charity Wright, analista de ameaça cibernética da IntSights:

> ...os bandidos, sejam cibercriminosos ou trabalhando para um governo, ou forças

[1]Doutoranda e Mestre em Estudos Estratégicos Internacionais pela Universidade Federal do Rio Grande do Sul - UFRGS. Atualmente é fellow no Alexander von Humboldt Institute for Internet and Society (HIIG). Contato:bruna.toso@ufrgs.br

> armadas, estão procurando a maneira mais fácil possível de obter acesso à rede e obter as informações de que precisam de seus adversários. Se isso significa usar o coronavírus e essa pandemia como uma atração, e esse é o ponto de entrada mais fácil, é definitivamente o que eles farão (WRIGHT apud GREIG, 2020, online, tradução nossa).

Dessa forma, os atores maliciosos usam de engenharia social para muitas vezes conseguir um *hop-point*, ou seja, um sistema com uma posição estratégica para comprometer sistemas adicionais dentro da rede alvo.

O acesso as redes alvo pode ser usado como parte de planos estratégicos de longo prazo, envolvendo campanhas de espionagem. De fato, relatórios do *Cyber Threat Intelligence Center* do grupo Thales[2] e a empresa de inteligência contra ameaças cibernéticas IntSights[3], mostram que vários grupos de hackers patrocinados pelo Estado estão usando o COVI-19 como parte de suas campanhas de espionagem. Os relatórios explicam que agentes mal-intencionados usam muitas vezes *phishing/spear-phishing* para atingir seus alvos. Em essência eles imitam uma fonte confiável e oferecem documentos supostamente contendo informações do COVID-19, atraindo seus alvos para a abertura desses documentos e, sem saber, baixando um malware oculto. Uma vez baixado, o malware fornece controle remoto do dispositivo infectado. Essas atividades envolvem atores que podem ser associados à Rússia (grupo Hades), China (Mustang e Vicious Panda), Coreia do Norte (Kimsuky) e Paquistão (APT36). Esses atores já afetaram alvos na Ucrânia, Taiwan, Vietnã, Mongólia, Coreia do Sul e Índia.

Esses resultados são relevantes, pois como alerta Buchanan (2020) o acesso às redes alvo pode gerar altas recompensas, que podem ser aproveitadas obtendo informações a nível militar, diplomático, industrial e de inteligência. Ademais, usando hackers para agir em seu nome, Estados conseguem se distanciar de responsabilidades ante a legislação internacional (ex. negação plausível), além de evitar conflitos diretos com seus alvos (MAURER, 2018).

Reações do mundo físico

Embora haja um baixo risco de retaliação para Estados patrocinando hackers em operações usais de espionagem cibernética, em tempos de COVID-19, as campanhas de espionagem se focam em informações sobre o vírus, fazendo com que as apostas estejam “mais altas” e potencialmente mudando essa tendência de baixo risco estatal. Segundo Sanger e Perlroth (2020) mais de uma dúzia de países reimplantaram hackers militares e de inteligência para recolher o que pudessem sobre as respostas de outras nações ao vírus. Diante do aumento de ataques cibernéticos, espionagem cibernética e desinformação no ciberespaço, o subsecretário-geral da ONU, Fabrizio

[2] A Thales é uma empresa global com operações em todos os continentes, atendendo a cinco principais mercados: aeroespacial, espacial, transporte terrestre, defesa e segurança e segurança digital. Ela possui o Estado francês como stakeholder, compreendendo 25.7% de de sua estrutura (THALES,2020)

[3] O IntSights é um empresa é de segurança cibernética orientada a inteligência que oferece inteligência rápida e precisa sobre ameaças cibernéticas e mitigação de incidentes em tempo real. Foi fundada em 2015 por ex-membros de uma unidade de inteligência de elite das Forças de Defesa de Israel (INTSIGHTS, 2020)

Hochschild (2020), pediu em abril um "cessar-fogo digital" global imediato durante a pandemia, e reações estatais começaram a proliferar.

O Reino Unido e os Estados Unidos já haviam emitido um comunicado conjunto, em 08 de abril, fornecendo informações sobre a exploração do COVID-19 por ameaças persistentes avançadas (normalmente ligadas aos Estados) (NCSC, CISA,2020a). Em 05 de maio, esses países lançaram novo comunicado para especificar que essas ameaças (APTs) estavam direcionando seus ataques cibernéticos a serviços essenciais e de saúde, mas não indicaram nos documentos nenhum país ou grupo de países ligados a essas atividades (NCSC, CISA, 2020b). Esse cenário mudou uma semana depois (no dia 13 de maio) quando os Estados Unidos acusaram formalmente a China pelo financiamento e operacionalização de células hackers que se infiltram em laboratórios de pesquisa trabalhando em respostas ao COVID-19 (FBI; CISA, 2020).

Pouco tempo após a acusação dos Estados Unidos, todos os países pertencentes a Aliança dos Cinco Olhos[4] pronunciaram-se em relação à espionagem por hackers patrocinados pelos Estados às instalações de pesquisa voltadas ao coronavírus. As agências de inteligência britânica MI6 e MI5 pediram que o governo repensasse suas relações com a China (DONNELLY, 2020). O Departamento de Relações Exteriores e Comércio australiano acusou, sem nomeação, países de conduzirem e apoiarem ataques cibernéticos sob a cobertura da crise do coronavírus (TILLET, 2020). As duas maiores agências de inteligência canadenses (*Canadian Security Intelligence Service* e *Communications Security Establishment*) expressaram que os atores patrocinados pelo Estado mudaram de foco durante a pandemia e que a propriedade intelectual canadense representaria um alvo valioso (TUNNEY, 2020). O Gabinete de Segurança das Comunicações (*Communications Security Bureau)* do Governo neozeladês pediu aos hackers que não alvejassem a pesquisa de coronavírus (BURROWS, 2020).

Além dessa movimentação, em reunião informal do Conselho de Segurança das Nações Unidas, transmitida via Youtube, no dia 22 de maio de 2020, todos os países da Aliança ressaltaram a aplicabilidade do direito internacional no ciberespaço e a aplicabilidade da estrutura criada a partir dos relatórios do Grupo de Peritos Governamentais das Nações Unidas no domínio da informação e das telecomunicações no contexto da segurança internacional (UNGGE), sobre o comportamento estatal responsável no ciberespaço. Nas declarações, os Estados Unidos reforçaram que haveria consequências caso os Estados não respeitassem a estrutura de comportamento estatal responsável (CHALET, 2020) e o Reino Unido enfatizou que atores hostis deveriam entender que "o comportamento estatal irresponsável no ciberespaço carregará um custo" (ROSCOE, 2020, p.1,tradução nossa).

Considerações finais

[4] Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia compõem a Aliança dos Cinco Olhos, que é uma coalizão de agências de inteligência independentes. (DAILEY, 2017)

Diante deste cenário, o que se pode constatar é que a acusação à China em particular, vai de encontro com a política de Trump de minar politicamente o país e responsabilizá-lo pelo momento vivido atualmente com a pandemia. Esse movimento pode ter grande repercussão para a China como fornecedora tecnológica, especialmente em se tratando de redes 5G, pois o país poderia perder mercados para concorrentes ocidentais e influência em várias partes do globo.

Assim, se por um lado as acusações podem levar a potenciais retaliações "offline", as quais podem não se restringir ao campo econômico e político, por outro lado, o movimento conjunto da Aliança dos Cinco Olhos direta ou indiretamente pode desencadear avanços legais necessários ao ciberespaço. Conforme Finnemore e Hollis (2019) acusações de ações cibernéticas bem construídas podem: (a) criar oportunidades para clarificar atuais leis de direito internacional e/ou criar novas leis que possam ser postas em prática para o âmbito digital; (b) compreender uma prática geral que mais tarde poderia ser aceita como *opinio juris*; (c) incitar Estados a desenvolverem uma instituição imparcial para atribuir ou advogar por direitos internacionais e (d) contribuir para considerações de instrumentos legais adicionais úteis para fazer essas acusações.

Qual cenário poderá se desenvolver ainda é incerto. Contudo, o que se pode apontar é que as ações e acusações feitas neste momento de pandemia, seja em particular à China ou a outros países, poderão contribuir de alguma forma para a formação de um "novo normal" mundial.

REFERÊNCIAS

BUCHANAN, Ben. **The Hacker and the State: Cyber Attacks and the New Normal of geopolitics.** Cambridge:Harvard University Press,2020

BURROWS, Matt. Coronavirus: **New Zealand's GCSB begs hackers not to target COVID-19 research after Chinese accused of cyber attacks**. 14 de maio de 2020. Disponível em: < https://www.newshub.co.nz/home/world/2020/05/coronavirus-new-zealand-s-gcsb-begs-hackers-not-to-target-covid-19-research-after-chinese-accused-of-cyber-attacks.html> Acesso em 25 de maio de 2020.

CHALET, Cherith Norman. **Remarks at a UN Security Council Arria-Formula Meeting on Cyber Stability and Responsible State Behavior in Cyberspace (via VTC**). 22 de maio de 2020. Disponível em:< https://usun.usmission.gov/remarks-at-a-un-security-council-arria-formula-meeting-on-cyber-stability-and-responsible-state-behavior-in-cyberspace-via-vtc/> Acesso em 25 de maio de 2020.

DAILEY, Jeffrey. The Intelligence Club: A Comparative Look at Five Eyes. [S.L] **Journal of Political Sciences & Public Affairs,** 5:261, June 2017. doi:10.4172/2332-0761.1000261

DONNELLY, Dylan. MI6 urges government to rethink China relationship after coronavirus pandemic. **Express**.13 de maio de 2020. Disponível em: < https://www.express.co.uk/news/weird/1268284/MI6-coronavirus-news-china-latest-intelligence-service-COVID-19-death-toll>. Acesso em 25 de maio de 2020.

FEDERAL BUREAU OF INVESTIGATION (FBI); CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). **People's Republic of China (PRC) Targeting of COVID-19 Research Organizations**. 13 de maio de 2020. Disponível em : < https://www.cisa.gov/sites/default/files/publications/Joint_FBI-CISA_PSA_PRC_Targeting_of_COVID-19_Research_Organizations_S508C.pdf.pdf> Acesso em 25 de maio de 2020

FINNEMORE, Martha; HOLLIS, Duncan B., Beyond Naming and Shaming: Accusations and

International Law in Cybersecurity. March 6, 2019. **European Journal of International Law** (forthcoming 2020); Temple University Legal Studies Research Paper No. 2019-14. Disponível em SSRN: http://dx.doi.org/10.2139/ssrn.3347958

GREIG, Jonathan. **Cybercriminals, state-sponsored groups ramping up attacks exploiting COVID-19 pandemic.** 08 de abril de 2020 disponível em : < https://www.techrepublic.com/article/cybercriminals-state-sponsored-groups-ramping-up-attacks-exploiting-covid-19-pandemic/> Acesso em 24 de maio de 2020.

HOCHSCHILD, Fabrizio. **To fight Covid-19, cyberattacks worldwide must stop immediately.** 10 de abril de 2020**.** Disponível em: < https://www.vox.com/world/2020/4/10/21216477/coronavirus-covid-19-pandemic-cyberattacks-digital-ceasefire-who-hack-united-nations> Acesso em 25 de maio de 2020.

INTSIGHTS. **Meet IntSights**. 2020. Disponível em: < https://intsights.com/company> Acesso em 24 de maio de 2020.

MAURER, Tim. **Cyber Mercenaries: The State, Hackers and Power**. Cambridge: Cambridge University Press, 2018

NAKAMITSU, Isumi. **Briefing at the Security Council Virtual Arria-formula meeting on "Cyber Stability, Conflict Prevention and Capacity Building**". 22 de maio de 2020. Disponível em: < https://front.un-arm.org/wp-content/uploads/2020/05/UNSC-Arria-Formula-Meeting-on-Cybersecurity-HR-Remarks-22-May-2020.pdf> Acesso em 25 de maio de 2020

NATIONAL CYBER SECURITY CENTER (NCSC); CYBERSECURITY INFRASTRUCTURE SECURITY AGENCY (CISA). **Advisory: COVID-19 exploited by malicious cyber actors**. 2020a. Disponível em: < https://www.ncsc.gov.uk/files/Final%20Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20v3.pdf > Acesso em 24 de maio de 2020.

NATIONAL CYBER SECURITY CENTER (NCSC); CYBERSECURITY INFRASTRUCTURE SECURITY AGENCY (CISA). **Advisory: APT groups target healthcare and essential services.** 2020b. Disponível em: < https://www.ncsc.gov.uk/files/Joint%20NCSC%20and%20CISA%20Advisory%20APT%20groups%20target%20healthcare%20and%20essential%20services.pdf> Acesso em 25 de maio de 2020

ROSCOE, James Paul. **Statement by Ambassador James Roscoe, UK Acting Deputy Permanent Representative to the UN, at the Security Council Arria formula meeting on Cyber Stability, Conflict Prevention and Capacity Building**. 22 de maio de 2020. Disponível em:< https://vm.ee/sites/default/files/Estonia_for_UN/statement_by_ambassador_james_roscoe.pdf> Acesso em 25 de maio de 2020.

SANGER, David E; PERLROTH, Nicole. U.S. to Accuse China of Trying to Hack Vaccine Data, as Virus Redirects Cyberattacks. **The New York Times**. 13 de Maio de 2020. Disponível em: < https://www.nytimes.com/2020/05/10/us/politics/coronavirus-china-cyber-hacking.html> Acesso em 25 de maio de 2020.

THALES. **About Us**. 2020. Disponível em: < https://www.thalesgroup.com/en/global/about-us> Acesso em 24 de maio de 2020.

TILLET, Andrew. Australia slams coronavirus crisis cyber attacks. **Financial Review**. 20 de maio de 2020. Disponível em:< https://www.afr.com/politics/federal/australia-slams-coronavirus-related-cyber-attacks-20200520-p54urp> Acesso em 25 de maio de 2020.

TUNNEY, Catharine. Increased foreign threat to COVID-19 research prompts extraordinary warning from Canada's spy agencies. **CBC News**. 14 de maio de 2020. Disponível em: <https://www.cbc.ca/news/politics/cse-csis-china-covid-1.5570134> Acesso em 25 de maio de 2020.