O mundo não está preparado para uma Ciberpandemia

Capitão (Reformado) Germán Afanador Ceballos,
Da Marinha da Colômbia

Alertas sobre os efeitos catastróficos que uma pandemia poderia gerar vinham sendo anunciados já há muitos anos por peritos na área. Bill Gates, entre outros, abordou esse tema em uma conferência do TED Talks.[1] Entretanto, na época, estadistas e líderes não deram muita atenção e prioridade para esses alertas da comunidade científica, de modo que recursos, ferramentas tecnológicas, análise preditiva e pessoal treinado não foram orientados para o devido acompanhamento do assunto. Foi apenas no início do ano de 2020, quando se sentiu o golpe devastador do seu efeito sobre a saúde pública, sua propagação incontrolável e o prejuízo sem precedentes para a economia, que os alarmes foram ativados, tardiamente – o que desencadeou uma série de medidas de reação em uma tentativa de estabilizar e amortecer o golpe recebido.

Algo muito semelhante ou em maior escala poderia surgir a curto prazo com os diferentes perigos que pairam no ciberespaço. Há tempos que se tem muitas advertências a esse respeito. Há vários *think tanks* reconhecidos e programas bem estruturados, patrocinados por grandes organizações, como a Organização das Nações Unidas (ONU), a Organização dos Estados Americanos (OEA), a União Europeia (UE), entre outras, dedicados ao tema. Entretanto, são poucos, entre os responsáveis pela tomada de decisões importantes, que entenderam a ameaça, muitas vezes relegando-a como um problema a ser resolvido pelos gerentes de tecnologia (TI) de instituições, agências e empresas. Esses alertas vêm aumentando exponencialmente, levando-se em conta que a nova normalidade com a qual se enfrenta a COVID-19 está agilizando a transformação digital a um ritmo acelerado, cujo objetivo é tratar de manter o fluxo da economia, em meio ao *tsunami* para o qual não se tinha um plano de mitigação previsto.

Desse modo, paralelamente às lições aprendidas com o manejo da pandemia, as ameaças do ciberespaço devem ser abordadas de forma holística e transversal e não apenas pelo encarregado da tecnologia ou segurança. Assim como contra o coronavírus, os governos, o setor produtivo e os acadêmicos uniram forças para tomar medidas preventivas e buscar soluções integrais, da mesma forma que são necessárias ações que permitam e facilitem de forma segura o bom uso do ciberespaço. Tal como através de fortes campanhas educativas as pessoas conseguiram

interiorizar que o autocuidado com o uso de máscaras, lavagem das mãos e o distanciamento social são fundamentais na mitigação de enfermidades virulentas, também é necessário que aqueles que se beneficiam da informática entendam que esse mesmo autocuidado seja assimilado, com o uso de senhas e suas frequentes mudanças, não acessando páginas inseguras, instalando antivírus e usando software licenciado, entre outros, que se tornam padrões mínimos básicos para a segurança cibernética, que são eficazes para mitigar o inimigo que persegue a todos no ambiente cibernético.

> Presidentes, Diretores Executivos (*Chief Executive Officers* – CEOs), militares e empresários não se deram por conta que é deles a responsabilidade de gerar estratégias de cibersegurança que se estendam a todos os níveis de suas equipes de trabalho e que a delegação aos responsáveis pela segurança e tecnologia os obriga a monitorar constantemente os protocolos, procedimentos e mecanismos com o objetivo de proporcionar os mais altos níveis de segurança às suas empresas. Analisar constantemente o futuro em busca de riscos é uma decisão prudente e madura por parte daqueles que têm a responsabilidade de garantir a segurança e a relevância de suas empresas. O que está acontecendo?

Ao tratar de temas de ciberdefesa e cibersegurança, existe uma percepção generalizada e equivocada de que somente compete a governos e megaempresas a busca pela proteção de suas infraestruturas críticas, grandes ativos e informações sensíveis. A verdade é que são muitos os exemplos de ciberataques ao redor do mundo, como por exemplo os da Estônia durante 2007 e os do *notPetya* e *WannaCry* em 2017, que deixaram em evidência não apenas os riscos apresentados pelo uso do ciberespaço com falhas de segurança, mas também as vulnerabilidades dos Estados e das multinacionais na forma como mitigam, tratam e se recuperam desse tipo de incidente. Fazendo uma analogia, esses ataques cibernéticos poderiam ser comparados às epidemias da Gripe Aviária, da Zika e do Ebola, que na época, levantaram bandeiras vermelhas de alerta. Porém, supôs-se tratar de questões concernentes apenas aos países do terceiro mundo, a serem abordados por cientistas, médicos altamente especializados e empresas farmacêuticas multinacionais.

A COVID-19 teve um impacto dramático sobre a população e forçou para que a sociedade, cada vez mais, dependesse da informática e ferramentas digitais que são sustentadas pela Internet. O que normalmente teria levado anos, hoje está sendo realizado em apenas alguns dias ou meses. A adoção em grande escala de tecnologias com acesso remoto que facilitam práticas de trabalho em domicílio, com uma maior dependência dos serviços na nuvem (*cloud*) permitiu às empresas a continuar com suas operações e reduzir alguns custos, cumprindo as ordens de confinamento decretadas pelos governos. No entanto, essas facilidades estão gerando um aumento notável nos riscos provenientes do ciberespaço.[2] O

coronavírus forçou empresas e indivíduos a passar por uma transformação digital às pressas, em menos de quatro meses, fazendo de 2020, forçosamente, o ano da transformação digital.[3] Não obstante, essa aceleração no espaço virtual, de tentativa e erro, está deixando brechas de segurança que estão sendo exploradas por cibercriminosos, especialmente porque os recursos alocados para a segurança eram limitados e uma porcentagem deles agora está sendo utilizada para lidar com a emergência pandêmica.

Essa pandemia nos ensinou quais são os verdadeiros pontos críticos e sensíveis da sociedade. Uma lição que terroristas e criminosos têm assimilado atentamente para o seu próprio benefício. Segundo relatórios da ONU, desde o surgimento da pandemia, a cada 39 segundos, há evidências de ataques cibernéticos a nível global. Da mesma forma, houve um aumento de cerca de 600% de e-mails maliciosos, bem como ataques cibernéticos consecutivos a organizações de saúde.[4] Outro informe do *Cyber Threat Intelligence League* indica que os *hackers* estão atacando em todos os níveis, tratando de roubar todas as informações possíveis, não apenas as relacionadas com o coronavírus.[5] De acordo com o informe *Managing the Impact of COVID-19 on Cyber Security,* desde o mês de janeiro próximo passado, quando a pandemia estava em sua fase inicial, temas relacionados com a COVID-19 foram usadas de forma massiva para disseminar, através do ciberespaço, *trojans* e *softwares* infectados com o fim de penetrar nos sistemas informáticos das empresas.[6] O centro médico de Parkview no Colorado, EUA, foi vítima de uma intrusão cibernética a seus sistemas de IT que o forçou a depender de histórias clínicas em papel, em pleno tratamento de pacientes com coronavírus.[7] Da mesma forma, alguns países estão aproveitando a COVID-19 para, através de ciberinteligência, se infiltrar nos sistemas governamentais e corporativos de outros Estados e realizar espionagem.[8] Recentemente, na Austrália, diferentes setores, tanto públicos como privados, foram vítimas de sofisticados assédios através do ciberespaço, supostamente provenientes de um estado hostil.[9] Ataques cibernéticos, como a curva da pandemia, têm se espalhado exponencialmente e parecem não encontrar um pico para começar a achatar; assim, poderia se dizer que um ataque cibernético com características semelhantes às do coronavírus seria capaz de se espalhar mais rapidamente e ter maior cobertura do que qualquer vírus biológico.[10]

Qual é o caminho a seguir?

A COVID-19 mudou por completo o estilo de vida da população mundial, acionou medidas biossanitárias, assim como novas regras e regulamentos. É evidente que enfrentar essa ameaça tem exigido um esforço conjunto. Portanto, é recomendável que instituições, organizações e empresas atualizem seus procedimentos de trabalho remoto enquanto verificam e reforçam suas políticas de segu-

rança informática pois a resiliência cibernética das empresas requer um esforço multidisciplinar combinado e alinhado na busca da coesão empresarial e na utilização de todas as oportunidades digitais.

Governantes, militares de alto cargo, CEOs e empresários devem levar em conta que definir e modelar o universo de ameaças que possam afetar sua organização é de sua inteira responsabilidade. No que diz respeito ao ciberespaço, para começar, há que se contar com a capacidade de detecção quando um adversário já infectou os seus sistemas. Em alguns casos demonstrados, pôde-se estabelecer que espiões cibernéticos são capazes de permanecer ocultos, por longos períodos de tempo, dentro dos sistemas de informática das empresas sem serem detectados, inclusive depois de terem sido realizadas inspeções internas de cibersegurança.[11] Acabar em uma unidade de terapia intensiva informática é devastador para uma organização; assim, o tratamento para a recuperação é ter uma equipe de especialistas (intensivistas) e agir o mais rápido possível. Estar preparado parece ser a melhor estratégia para sustentar a economia dos países em uma iminente pandemia cibernética.

Paralelamente, como na pandemia, é necessário proteger os grupos de risco, adotando abordagens proativas de cibersegurança que identifiquem efetivamente as vulnerabilidades nos sistemas antes que elas sejam comprometidas. Isso só é possível fazendo um amplo monitoramento das redes, praticando o *hacking* ético, fazendo treinamento constante de todo o pessoal e realizando auditorias de segurança cibernética por especialistas completamente independentes da organização.[12]

Ao desenvolver planos de mitigação de riscos, deve ficar claro que a cibersegurança atravessa todos os processos da empresa. A cibersegurança sozinha em uma organização fica aleijada. É imprescindível que todo empregado, independentemente do seu nível na empresa, que tenha acesso a um computador, um *tablet* ou um *smartphone*, deve entender que processar dados e arquivos, através de meios informáticos, os torna potencialmente suscetíveis a serem sabotados, roubados e espionados - portanto, deve-se ter o treinamento e supervisão adequados para evitar este tipo de incidente. Do contrário, há um alto risco de pôr em perigo o capital informático, o prestígio e as informações confidenciais da organização ou empresa onde trabalha. Portanto, é extremamente importante contar com talento humano qualificado e constantemente realizar campanhas educacionais em todos os níveis da organização.

Conclusões

Se algo permitiu manter a infraestrutura crítica e a economia em meio a esse furacão, é a Internet, a virtualidade e o trabalho remoto. A não adoção de medidas preventivas, em tempo hábil, em termos de regulamentação e bom uso do ciberes-

paço, poderia desencadear um surto cibernético que levaria a sociedade a uma ciberquarentena prolongada, enquanto dados, arquivos, programas são recuperados e os sistemas infectados, alterados ou bloqueados são corrigidos. Situação essa que seria seguramente mais catastrófica do que a que vivemos na atualidade. ❑

Notas

1. Bill Gates. ¿La próxima epidemia? No estamos listos. https://www.ted.com/talks/bill_gates_the_next_outbreak_we_re_not_ready?language=es
2. Cybersecurity Leadership Principles. Lessons Learned During the COVID 19 Pandemic to Prepare for the New Normal. World Economic Forum. May 2020.
3. Enrique Dans. La Crisis del Coronavirus y el Darwinismo Digital. https://www.enriquedans.com/2020/04/la-crisis-del-coronavirus-y-el-darwinismo-digital.html.
4. Izumi Nakamitzu. Alta Representante de la ONU para asuntos de Desarme. https://forbes.co/2020/05/22/actualidad/se-calcula-que-hay-un-ataque-informatico-en-el-mundo-cada-39-segundos-onu/.
5. They are trying to steal everything. US Coronavirus response hit by foreign hackers. https://edition.cnn.com/2020/04/25/politics/us-china-cyberattacks-coronavirus-research/index.html
6. Managing the Impact of Covid-19 on Cyber Security. Março 2020. https://www.pwc.es/es/covid-19/ciberseguridad-gestionar-impacto-covid19.html.
7. Bulletin on recent ransomware and disruptive attacks. The Chertoff Group. Junho 2020
8. Cybercrime, Threats Turing the COVID 19 pandemic. Global Initiative against transnational organizad crime. Abril 2020, pag 10.
9. The Guardian. Cyber Attack Australia: Sophisticated attacks from state based actor. https://www.theguardian.com/australia-news/2020/jun/19/australia-cyber-attack-attacks-hack-state-based-actor-says-australian-prime-minister-scott-morrison.
10. What Covid 19 Pandemic teaches us about cybersecurity. World Economic Forum. https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/.
11. El colombiano que vendió una multinacional de ciberseguridad y creo una nueva que esta volando. Revista Forbes. https://forbes.co/2020/07/06/emprendedores/ricardo-villadiego-vigilante-de-la-red/.
12. Proactive Vs Reactive Cybersecurity. Experts opinions. https://www.vpnranks.com/blog/proactive-vs-reactive-cybersecurity-expert-opinions/.

Capitão (Reformado) Germán Afanador Ceballos, Da Marinha da Colômbia

Capitão aposentado da Marinha da Colômbia, consultor de negócios, palestrante, bastante experiência em questões de segurança cibernética, análise de risco e planejamento estratégico com 30 anos de experiência. Estudos na Colômbia e no exterior relacionados com Engenharia Naval Eletrônica, Ciências Navais, pós-graduação em Segurança, Defesa Nacional, Estudos Políticos e Mestrado em Estudos Estratégicos de Segurança.

Sua experiência se baseia na implementação de planos de segurança e continuidade de negócios para proteção de ativos e desenvolvimento de funções críticas; gestão de estudos, auditorias de segurança e informação e convênios com órgãos locais e internacionais visando o fortalecimento de capacidades empresariais. Assessoria a Conselhos de Administração de empresas privadas, em questões estratégicas e de segurança. Excelente liderança e orientação de grandes grupos de pessoas para o cumprimento dos objetivos estratégicos.