The World is not Prepared for a Cyber Pandemic

CAPT (Ret.) Germán Afanador Ceballos,
Colombian Navy

For years, alerts about the catastrophic effects that a pandemic could generate have been announced by experts on the subject. One such expert, Bill Gates, in 2015, addressed this subject at a TED Talks conference.[1] However, at the time, neither statesmen nor leaders paid much attention or prioritized the scientific community's cries for action. Resources, technological tools, predictive analysis, and trained personnel were not prepared to monitor the issue properly. It was not until 2020—when the devastating blow of the pandemic's effect on public health, the uncontrollable spread, and the never-before-anticipated damage to the economy was felt—that the alarms were belatedly activated. A whole series of reactive measures were unleashed—seeking to stabilize and buffer the blow received.

Something remarkably similar or on a larger scale could happen in the short term because of the different dangers that haunt cyberspace. We have received many warnings in this regard. There are various prestigious think tanks and systematic programs sponsored by immense organizations, such as the United Nations (UN), the Organization of American States, and the European Union, among others, that are dedicated to the subject. However, not many of those decision-makers understand the threat. It is often relegated as a problem that must be solved by Information Technology (IT) managers of institutions, organizations, and companies. These alerts have been increasing exponentially. They now realize that COVID-19 is hastening the digital transformation at an accelerated rate. Trying to keep the economy afloat amid the tsunami was not contemplated as part of the mitigation plan.

Thus, by comparing the lessons that the management of the pandemic has left us, cyberspace threats must be faced in a holistic and transversal way and not just by the person in charge of technology or security. Like the fight against the Coronavirus, governments, the private sector, and academia have joined forces. They are taking preventive measures and seeking comprehensive solutions that allow and safely facilitate cyberspace's proper use. Similarly, through strong educational campaigns, people have internalized self-care with masks, hand washing, and social distancing, which are fundamental in mitigating this virus. Those who benefit from

computing must understand the importance of this same self-care. This will be accomplished by changing passwords frequently, not accessing insecure sites, having antivirus licensed software. These efforts are the bare minimum cybersecurity standards that effectively mitigate the enemy that stalks everyone from cyberspace.

Presidents, Chief Executive Officers (CEOs), the military, and business professionals have not understood that it is their responsibility to generate cybersecurity strategies that reach all their work team levels. Delegating those in charge of security and technology with this responsibility forces them to continually supervise protocols, procedures, and mechanisms to provide the highest security levels to their companies. Constantly analyzing the future in search of risks is a prudent and mature decision for ensuring their companies' safety and importance. What is happening?

In dealing with cyber defense and cybersecurity issues, there is a generalized and mistaken perception that it only concerns governments and mega-companies that seek to protect their critical infrastructures, large assets, and sensitive information. The truth is that there are many examples of cyberattacks around the world. For instance, Estonia during 2007, and *NotPetya* and *WannaCry* in 2017. These attacks revealed the risks posed to using cyberspace with gaps in security issues and the vulnerabilities of countries and multinationals when they mitigate, confront, and recover from these types of incidents. These cyberattacks could be compared to the Avian Flu, Zika, and Ebola epidemics. At that time, these diseases raised red flag warnings but were believed to be matters only for third-world countries and that they should be addressed by scientists, highly specialized doctors, and multinational pharmaceutical companies

COVID-19's dramatic impact has forced society to increasingly depend on information technology and digital tools supported on the Internet. Tasks that usually would have taken years are now being accomplished in just days and months. The large-scale adoption of remote access technologies that facilitate work-from-home, with greater dependence on cloud services, has allowed companies to continue their operations, reduce costs, and comply with the governments' decreed confinement orders. However, these facilities are also generating a notable increase in risks from cyberspace.[2] The Coronavirus has forced companies and individuals to undergo a sudden digital transformation in fewer than four months—forcibly making 2020 the digital transformation year.[3] However, by trial and error, this acceleration in virtual space is leaving security gaps that are being exploited by cybercriminals. This is especially evident if one considers that the resources allocated for security were insufficient. Furthermore, some percentages of those resources are being used to take care of the emergencies caused by the pandemic.

This pandemic has taught us the genuinely critical and sensitive nature of society's data usage: a lesson that terrorists and criminals have quickly learned for their benefit. According to UN reports— since the emergence of the pandemic— every 39 seconds, there is evidence of cyberattacks globally. Likewise, malicious emails have increased by 600 percent, and consecutive cyberattacks against health organizations have been perpetrated.[4] Another report from the Cyber Threat Intelligence League indicates that hackers are attacking at all levels and attempting to steal all possible information, not just Coronavirus-related information.[5] According to the Managing the Impact of COVID-19 on Cyber Security report, data and information related to COVID-19 were used en masse through Trojans during this past January. Trojans infected software and penetrated companies' computer systems.[6] The Parkview Medical Center in Colorado was the victim of a cyber intrusion. It resulted in its IT systems being forced to depend on paper medical records in the middle of treating patients with Coronavirus.[7] Other countries are also taking advantage of instability during COVID-19 to infiltrate other states' government and corporate systems. This is completed by obtaining cyber intelligence and carried out via espionage.[8] Recently, various public and private sectors in Australia were victims of sophisticated cyber harassment, which allegedly came from a hostile state.[9] Cyberattacks, like the curve of the pandemic, have been spreading exponentially and are not peaking and then flattening out. Therefore, it could be said that a cyberattack with characteristics like those of the Coronavirus would spread faster and have more significant exposure than any biological virus.[10]

What Path Do We Follow?

COVID-19 completely changed the lifestyle of the world's population, triggered bio sanitary measures, and established new rules and regulations. Facing this threat has required a joint effort. Institutions, organizations, and companies must update their remote work procedures while verifying and enforcing their IT security policies. This is because the cyber resilience of companies requires a combined and aligned multidisciplinary effort. It must focus on business cohesion and take advantage of all digital opportunities

Governments, high-ranking military personnel, CEOs, and people in business must bear in mind that defining and modeling the universe of threats that can affect their organizations is their utmost responsibility. First, it is necessary to have the ability to detect when an adversary has already infected a system. It has been proven that cyber spies can remain hidden for extended periods within companies' computer systems without being detected. This occurs even after internal cybersecurity inspections have been carried out.[11] Ending up in a computer "in-

tensive care unit" is devastating for an organization. The treatment plan includes having an expert team (specialized in intensive cybersecurity care) and acting as quickly as possible. Being prepared seems to be the best strategy to sustain countries' economies during this imminent cyber pandemic.

Similar to the pandemic, with cybersecurity, it is necessary to protect risk groups by adopting proactive approaches that effectively identify vulnerabilities in systems before they are compromised. This is only achieved by carrying out extensive monitoring of networks, practicing ethical hacking, continually training all staff, and conducting cybersecurity audits by nonaffiliated independent experts.[12]

When preparing risk mitigation plans, it must be clear that cybersecurity is linked to all company processes. Cybersecurity operating independently of an organization is ineffective. It is essential that every worker—regardless of their level in the company and who has access to a computer, tablet, or smartphone—understand that processing data and files through automated means makes them potentially susceptible to being sabotaged, stolen, and spied upon. Therefore, one must have proper training and supervision to avoid these types of incidents. Otherwise, there is a high risk of endangering the IT capital, prestige, and classified information of the organization or company at which one works. Therefore, it is imperative to have a qualified and talented workforce that can continuously carry out educational campaigns at all organizational levels.

Summary

The Internet, virtual reality, and working remotely have allowed critical infrastructures and the economy to be maintained during this pandemic. Failure to promptly take preventive measures regarding the regulation and proper use of cyberspace could trigger a cyber outbreak that could lead society to plunge into a prolonged cyber quarantine. Simultaneously, data, files, and programs can be recovered, and the infected, altered, or blocked systems are corrected. This situation would surely be more catastrophic than the one we live in today. ❑

Notes

1. Bill Gates. The next epidemic? We are not ready. https://www.ted.com/talks/bill_gates_the_next_outbreak_we_re_not_ready?language=es

2. Cybersecurity Leadership Principles. Lessons Learnd 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 (The Coronavirus crisis and the digital Darwinism). https://www.enriquedans.com/2020/04/la-crisis-del-coronavirus-y-el-darwinismo-digital.html

4. Izumi Nakamitzu. UN High Representative for Disarmament Matters. 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. Marzo 2020. https://www.pwc.es/es/covid-19/ciberseguridad-gestionar-impacto-covid19.html.

7. Bulletin on recent ransomware and disruptive attacks. The Chertoff Group. June 2020.

8. Cybercrime, Threats during the COVID 19 pandemic. Global Initiative against transnational organized crime. April 2020, page 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 está volando (The Colombian that sold a cybersecurity multinational and created a new one that is rapidly growing. Forbes Magazine. 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/

CAPT (Ret.) Germán Afanador Ceballos,
Colombian Navy

Business Consultant, Lecturer—30 years of experience in cybersecurity, risk analysis and strategic planning. Postgraduate degrees in Security, National Defense, and Political Studies; Master's degree in Strategic Security Studies; and studies in Colombia and abroad related to Electronic Naval Engineering and Naval Science. Experience implementing security and business continuity plans for asset and critical functions protection; security and information audits with local and international agencies aimed at strengthening corporate capabilities. Advisor to Boards of Trustees of private companies on strategic and security issues. Outstanding leadership and guidance to large organizations towards achieving strategic objectives.