VOLUME 9, ISSUE 1, 2018

per Concordiam

Journal of European Security and Defense Issues

- **CYBER WARFARE IN UKRAINE**
  The Russian doctrine behind the attacks
- **BUILDING DIGITAL DEFENSES**
  Public-private partnerships are vital
- **THE POWER OF RESILIENCY**
  Thwarting today's 24/7 onslaught
- **UTILIZING STRATEGIC FORESIGHT**
  Taking steps to secure cyberspace

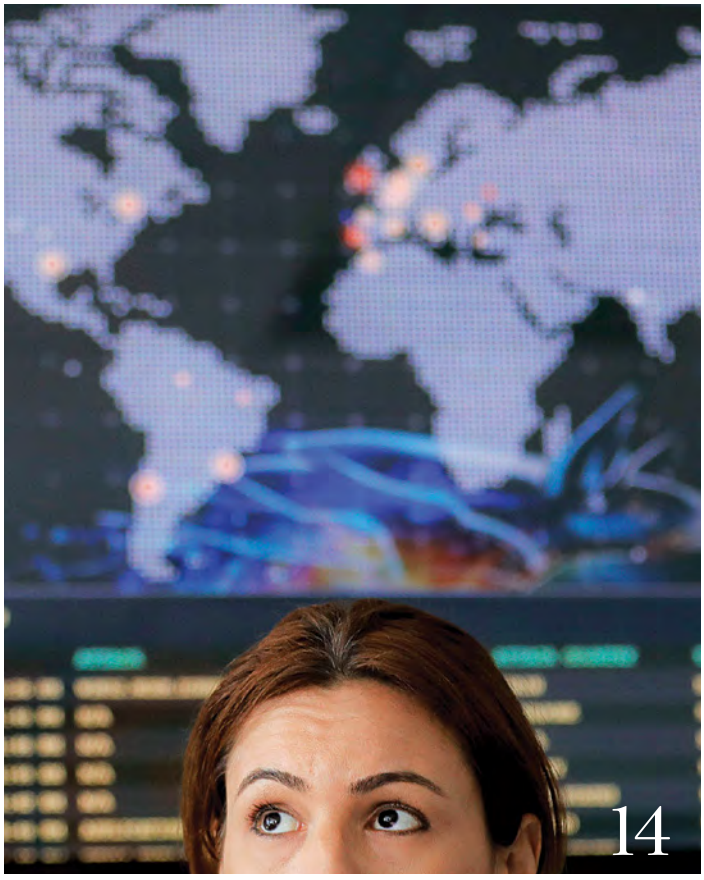
PLUS

The case for a cyber reserve force in Georgia
Hardening the Czech Republic against assaults
Kosovo's rapid internet growth brings challenges

MISSION CRITICAL

Protecting Essential Infrastructure from Cyber Attacks

features



departments

in every issue

SECURITY

POLICY

COOPERATION

on the cover:

Plotting a defense against the escalating number and intensity of cyber attacks requires planning, teamwork and execution.

ISTOCK

GEORGE C. MARSHALL
EUROPEAN CENTER FOR SECURITY STUDIES

Welcome to the 33rd issue of *per Concordiam*. This special cyber edition covers a wide range of cyber security topics with a common thread: how best to protect critical infrastructure in the face of increasingly sophisticated threats by states and by state-sponsored and nonstate actors. The sophistication level of cyber threats to national security has increased exponentially over the past few years. Regionally and throughout the world, these challenges differ based on the penetration level of internet and mobile communications and the unequal distribution of expertise in given areas. As such, the overlaying, global nature of cyberspace makes examining real-world case studies and trends equally vital.

Cyber crime remains one of the greater transnational threats, and it is primarily motivated by the opportunity for considerable financial gain. In 2017, ransomware, such as WannaCry, showed just how vulnerable modern, information technology-dependent societies are to criminal enterprises. North Korea was implicated as the source of WannaCry, which encrypted enterprise and personal data and held it for ransom.

Other countries, notably Russia, are actively involved in mapping the energy grids and fiber-optic systems of potential adversaries, presumably as a means for gaining geopolitical advantage. Experts agree that the events in Ukraine have become a testing ground for cyber and its asymmetric use. Critical infrastructure manipulation as a force-multiplying tool was evident in Ukraine, replete with industrial control system-induced blackouts in Kyiv, interference with the nation's financial system and other ransomware, such as NotPetya.

Cyber security is increasingly recognized as not merely a governmental function, but one that benefits from cooperation between the public and the private sectors. Many facets of critical infrastructure, including supply-chain vulnerabilities and encryption challenges, have a significant private-sector component.

This edition includes notable contributions from subject-matter experts and cyber professionals from across the world, whose articles explore cyber security shortfalls in critical infrastructure and provide fresh ways to approach solutions for protection and resiliency. Readers will enjoy articles covering the establishment of effective public-private partnerships, information sharing to enhance cyber security risk management and resilience, and the irreplaceable role of diligent cyber strategy creation, policy development and properly established legal frameworks to minimize cyber risk.

The Marshall Center's Program on Cyber Security Studies (PCSS) is a premier program that emphasizes strategy and planning within the framework of whole of government, public-private partnerships and transnational cooperation. PCSS imparts an appreciation of the cyber ecosystem and the magnitude of today's threats. In so doing, PCSS develops a common understanding of the lexicon, best practices and current cyber initiatives within the public and private sectors.

It is my pleasure to provide the introduction to this cyber edition of *per Concordiam* and to recognize all of this issue's contributors, many of whom are PCSS alumni. We welcome your comments and perspectives on these articles and opinions and look forward to continuing the dialogue in future cyber editions of this journal. Please feel free to contact us at editor@perconcordium.org

Sincerely,

Keith W. Dayton
Director

Keith W. Dayton
Director, George C. Marshall European Center for Security Studies

Keith W. Dayton retired as a Lieutenant General from the U.S. Army in late 2010 after more than 40 years of service. His last assignment on active duty was as U.S. Security Coordinator to Israel and the Palestinian Authority in Jerusalem. An artillery officer by training, he also has served as politico-military staff officer for the Army in Washington, D.C., and U.S. defense attaché in Russia. He worked as director of the Iraqi Survey Group for Operation Iraqi Freedom in Iraq. He earned a Senior Service College Fellowship to Harvard University and served as the Senior Army Fellow on the Council on Foreign Relations in New York. Gen. Dayton has a bachelor's degree in history from the College of William and Mary, a master's degree in history from Cambridge University and another in international relations from the University of Southern California.

Hafize Bajrami has been chief of the information technology (IT) section in the Ministry for the Kosovo Security Forces since 2009 and a member of the Kosovo National Cyber Security Council since 2016. She holds a master's degree in telecommunications from the University of Pristina and spent two years as an IT engineer in the private sector. She is an alumna of the Marshall Center, where she attended the Program on Cyber Security Studies and a Cyber Security Community of Interest event in 2017.

Lt. Col. Darko Galinec, Ph.D., is head of Croatia's Information Systems Security and Control Section in the Sector of Information and Communications Systems of the Ministry of Defence. He has held many positions in the ministry's information and communications systems, including those responsible for upholding NATO's Cyber Defence Pledge. He graduated from the Marshall Center Program on Cyber Security Studies. His research focus areas are cyber security and cyber defense.

Andria Gotsiridze was director of the Cyber Security Bureau of the Ministry of Defence of Georgia from 2014 to 2016. He was the ministry's inspector general with an expertise in security sector reform, fighting corruption and foreign intelligence. Under his leadership, the ministry's Cyber Security Bureau developed Georgia's first cyber security defense policy and strategy and initiated a number of security projects. He is currently involved in several projects as a cyber security advisor at the Georgia Innovation and Technology Agency.

Martin Konečný is an analyst in the National Cyber and Information Security Agency of the Czech Republic, where he is responsible for the Department of Regulation and Audits. He received his master's degree from Brno University of Technology. His expertise is in information security management systems.

Col. Viktor Lisakonov is head of the Information Assurance Directorate within the General Staff of the Ukrainian Armed Forces. He helped establish the Ukrainian military Information Assurance and Cyber Defence System. During a 30-year career he has held various command and staff positions and has experience with peacekeeping operations. His current focus is on developing military cyber defense capabilities.

Maka Petriashvili has worked at the Ministry of Defence of Georgia since 1999, specializing in cyber security, military intelligence, defense policy and planning, human resources and strategic defense review. She worked as a human resources and organizational development consultant in the Cyber Security Bureau and coordinated the Cyber Security Awareness Project in 2015-2016. She is also involved with cyber security awareness training and has participated in the development of NATO's Cyber Security Generic Reference Curriculum. She holds a master's degree in security studies from the U.S. Naval Postgraduate School in Monterey, California, and a master's degree in human resource management from the University of Manchester, England.

Capt. Domingos Tavares has been deputy director of intelligence services for Cape Verde since 2013. After enlisting in the military in 1997 as an artillery squad leader, he became a commissioned officer in 2000. He earned a bachelor's degree in mathematics and statistics at Cape Verde University and has completed officer training courses at the United States Army Military Police School at Fort Leonard Wood, Missouri, the Military Intelligence Basic Officer Course Africa in Senegal, and the Anti-Terrorism/Anti-Piracy Course at the U.S. Naval Air Station in Pensacola, Florida. He attended a Countering Transnational Organized Crime program at the Marshall Center.

Maj. Walbery Nogueira de Lima e Silva of the Brazilian Army is staff officer at the country's Cyber Defense Command. He served as commander of the 2nd Army Signal Company from 2012 to 2013 and chief of the Cyber Operations Division of the Brazilian Cyber Defense Center in 2016. Walbery has attended German Armed Forces and NATO System of Command and Control courses and the Marshall Center's Program on Cyber Security Studies.

Agnieszka Wierzbicka is an expert on cyber security, international relations and media. She has advised speakers of the Polish Parliament, Polish and German presidents and the plenipotentiary of the Polish minister of digital affairs for cyber security. Wierzbicka is helping to implement the European Parliament's network and information systems directive, has contributed to the Polish cyber security strategy and coordinates the Polish government's participation in the European Cybersecurity Organization. She studied political science at the universities of Warsaw, Constance and Bonn.

per Concordiam
Journal of European Security and Defense Issues

Cyberspace: Protection of Critical Infrastructure

Volume 9, Issue 1, 2018

Contact Us

per Concordiam editors
Marshall Center
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany
editor@perconcordiam.org

per Concordiam is a professional journal published quarterly by the U.S. European Command and the George C. Marshall European Center for Security Studies that addresses defense and security issues in Europe and Eurasia for military and security practitioners and experts. Opinions expressed in this journal do not necessarily represent the policies or points of view of these institutions or of any other agency of the German or United States governments. Opinions expressed in articles written by contributors represent those of the author only. The secretary of defense determined that publication of this journal is necessary for conducting public business as required of the U.S. Department of Defense by law.

ISSN 2166-322X (print)
ISSN 2166-3238 (online)

PER CONCORDIAM ILLUSTRATION

Lessons from UKRAINE

Russia's multilayered cyber assaults know no bounds

By **Col. Viktor Lisakonov**, chief of the Information Assurance Directorate, Ukrainian General Staff

Innovation has driven military strategy since the dawn of humanity. The inventions of gunpowder, the rifle-barreled gun and the combustion engine had huge impacts not only on military strategy, but on all of history. The 20th century was no exception. The evolving internet continues to expand the capacities of information technologies. But, as with other great inventions, its capabilities have frequently been used for negative purposes. The first computer viruses were created just for fun, but served as a warning for some and a criminal road map for others — cyber espionage, cyber attacks and identity theft are common now. However, there is a new aspect to the cyber threat.

On December 23, 2015, unknown hackers disconnected about 30 electrical substations in Ukraine, cutting power for about 250,000 people in the middle of a freezing winter. Before that night, no one had ever used cyber attacks against civilian critical infrastructure without an obvious monetary benefit. We now face a new threat with tremendous military and geopolitical potential. Within a short span of time, a single exploitation of systems vulnerabilities has evolved into an effective toolkit of hybrid capabilities with which to pursue a given geopolitical agenda. This reflects the new operational environment of cyber warfare, as Russia has demonstrated, using it to gain military and overall superiority in current and prospective conflicts. Understanding the threats, especially in their initial phase, serves a crucial role in choosing a successful response.

The notorious Gerasimov Doctrine was set forth in 2013 by Russia's chief of general staff, Gen. Valery Gerasimov, in "The Value of Science Is in the Foresight," published in the weekly Russian newspaper *Military-Industrial Courier*. This doctrine, which Russia implemented in Ukraine with oversight by Vladislav Surkov, a personal adviser to Russian President Vladimir Putin, implies the creation of chaos, inconsistency and internal conflicts. While instability and chaos-induction are not new to the Russian model of conflict resolution, Gerasimov and Surkov adapted it for implementation in the ongoing hybrid aggression against Ukraine. The use of cyber means, synchronized with a powerful propaganda base, political pressure and broad-spectrum military application, has been effective in causing instability in Ukraine.

From the beginning of the annexation of Crimea through the follow-on Russo-Ukrainian conflict in the eastern part of Ukraine, cyber operations accompanied all phases of aggression, especially kinetic operations. "In Ukraine, Russia has experimented with how best to produce military and political benefits from cyber

Masked Russian soldiers, also known as "green men," move toward a military base in Perevalnoe, Ukraine, in March 2014 after invading Ukraine's Crimean Peninsula. GETTY IMAGES

operations," Kenneth Geers explains in his book, *Cyber War in Perspective: Russian Aggression Against Ukraine*. In *Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy*, James J. Wirtz describes the role of the cyber domain in Russian strategy: The "Russian Federation seems to have devised a way to integrate cyber warfare into a grand strategy capable of achieving political objectives." Key points for exploitation are lack of international legislative maturity, the complexity of the cyber domain and inherent anonymity. This approach allows the conduct of any manner of cyber operations to affect a harmful impact while leaving few traces or concrete evidence of Russian presence.

Throughout four years of Russian aggression, Ukraine has been under the constant pressure of cyber attacks in almost all spheres of life. However, attacks on critical infrastructure have evolved to be among the most dangerous and efficient in terms of potential and social impact. Seventeen years ago, security expert Bruce Schneier described a paradigm shift in his book, *Secrets and Lies: Digital Security in a Networked World*, which features a massive military application of civil technologies and infrastructure in place of conventional military assets. Use of the same computer systems by civilians and militaries implies that the same attack used against civilian targets could also be used against military targets. Given what has taken place in Ukraine, it is evident that attacks on critical infrastructure are among the most dangerous threats today.

Two Russian soldiers, captured in the conflict zone in eastern Ukraine, stand trial in Kyiv in September 2015 on terrorism charges. REUTERS

Bureaucratic challenges

Perhaps the trickiest challenge of attacks on critical infrastructure is the immaturity of international legislation regarding cyber security and collective defense. Due to the relative novelty of the cyber domain, there is no appropriate legislative basis or vetting mechanism for the punishment of cyber criminals. An adversarial action requires an appropriate and proportional response, but a working mechanism for executing such a response does not currently exist.

A Ukrainian Armed Forces' cyber analyst scrutinizes NotPetya images in 2017. COL. VIKTOR LISAKONOV

Passengers wait to check their luggage at Boryspil International Airport outside Kyiv in 2017. The NotPetya cyber attack caused significant disruptions to business and daily routines in Ukraine. REUTERS

NATO's Article 5 implies that aggression against one member shall be met with a response by all members, including the potential use of armed force. As of July 2016, the Alliance began to recognize cyberspace as a domain of operations equal to air, land and sea. This means that an attack on any of the allies in cyberspace is grounds for a response, possibly an armed one. However, in the case of cyber attacks, attribution can be very difficult and complicated. How do you prove a suspect was the attacker? What evidence should be required? What types of attacks could be grounds for an armed response from the entire organization? Does NATO have procedures for handling these situations? A response option likely exists, but any decision could be rejected by one or more members. There are more questions than answers. That is why — across roughly 10 years of cyber attacks on critical infrastructure systems during geopolitical confrontations (starting with a massive series of attacks on Estonian public and private sector institutions in 2007) — there has been no solid precedent for officially attributing an attack to an attacker or means by which to punish an attacker.

This lack of clarity contributes to the increasing number of cyber attacks, and some nations successfully use this ambiguity to reach their geopolitical or military goals. Even though we traditionally think of critical infrastructure as civilian assets, hackers will not differentiate between civilian and military objects. In other words, cyber attackers will likely continue to take aim at critical infrastructure targets, regardless of whether the target is labeled civilian or military.

In addition, global security systems are based on coordinated responses to aggression. That means involving an international security body that discusses the problem, and then votes on and executes procedures. All of this consumes a crucial resource: time. Due to the nature and purpose of critical infrastructure, such long response times could bear too high a cost, such as humanitarian or ecological catastrophes resulting in the loss of innocent lives and destroyed environments. Such potentially disastrous impacts require imminent changes to response procedures.

According to the Law of War as defined by the Geneva Conventions (and subsequently, by the Protocol Additional to the Geneva Conventions of August 12, 1949, and Protocol I of June 8, 1977), any attacks against objects of civilian infrastructure are strictly prohibited. These rules imply that attacks on civilian infrastructure include cyber attacks, although this has yet to be specifically spelled out within the Geneva Conventions. Potential anonymity in the cyber domain, along with legislative immaturity, provide free rein to groups and even state actors to operate in cyberspace with no punishment or regulatory consequences. The worst-case scenario would be civilian critical infrastructure being targeted to gain military superiority.

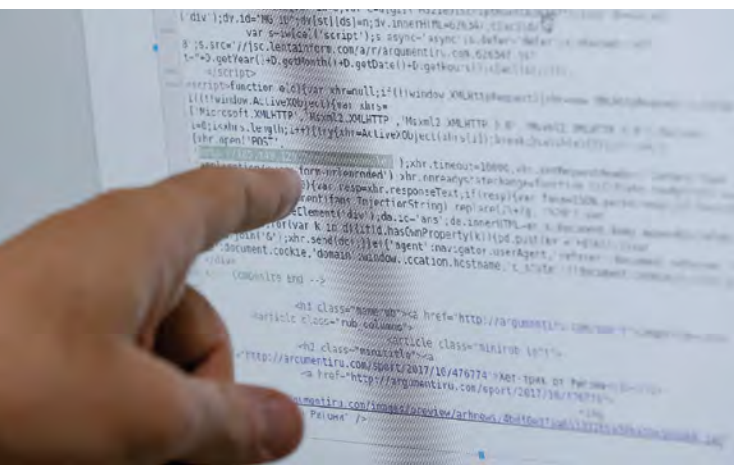
Growth of cyber attacks

After the "rebirth" of the Ukrainian Armed Forces, which included a significant increase in defensive capabilities and front-line stabilization, Russian cyber attacks became increasingly prominent in maintaining hybrid pressure on Ukraine. Not long ago, few could imagine causing the collapse of transportation infrastructure or cutting off a city's electricity in pursuit of geopolitical aims. Previously, only terrorist attacks were considered threatening to critical infrastructure, in the form of improvised explosive devices or similar conventional weapons. But now, the targeting of critical infrastructure via cyber means during a geopolitical confrontation is a reality. Ukrainian critical infrastructure assets have been attacked about a dozen times over a two-year period.

The most significant examples of such attacks include a citywide blackout in Kyiv, an attack on the western Ukrainian power grid, and attacks on Ukraine's treasury, Finance Ministry and railway administration and,

of course, the NotPetya malware attack. It is important to note that all of these attacks mainly targeted civilians rather than military or government installations. The aim was to affect ordinary people in their daily routines by blocking ATMs, disrupting business processes and so forth. For instance, the treasury and railway administration hacks caused noticeable financial loss and transport delays. Practically none of the financial losses were incurred by the government, but there were problems for regular people who were not able to get tickets or money at Christmastime. These destabilization efforts were intended to degrade and handicap Ukraine from within.

The NotPetya attack was a massive campaign that affected the entire country through money losses, transport collapse, acts of intimidation and data leakage. The deep-dive analysis revealed its complex and multilayered nature, with a high cyber-component ratio. The extreme complexity, multilayered nature and coordination of the NotPetya campaign exposed the magnitude of state-level support for the malware attack. This campaign was not just an espionage campaign, nor just an operation to induce financial loss, nor a psychological operation. This was the practical use of cyber warfare as a major component of a hybrid operation, which in turn, is an implementation of the Gerasimov Doctrine. The takeaway from the NotPetya campaign is that cyber warfare dominance played an extremely important role in attaining superiority in this geopolitical confrontation.



A Ukrainian Cyber Police employee points to a malicious script used during a virus attack in 2017. REUTERS

In accordance with the Gerasimov Doctrine, Russia has intensively developed and widely used offensive cyber capabilities. A major part of these capabilities is directed toward critical infrastructure in order to affect ordinary people, making their lives more difficult and creating mass discontent. The main objective is to exploit a dominant cyber warfare position to gain advantage during geopolitical clashes. The approaches used in Ukraine could and probably will be used against Russia's other geopolitical opponents. In this respect, one of the main priorities is to protect critical infrastructure against cyber attacks. Adding to this is the challenge of preparing ordinary citizens for the near-certainty that they will be targeted in the event of a geopolitical confrontation.

Increasing severity, sophistication

The concept of using cyber attacks in a European country should be assessed in terms of whether such attacks are effective means for achieving geopolitical objectives. There has been an increase in the number, severity and sophistication of these attacks. For instance, during the Russo-Georgian War in August 2008 to disrupt communication between the Georgian government and citizens, Russian military cyber groups employed primarily low-technology distributed-denial-of-service (DDoS) attacks. Six years later, during Russia's occupation of the Crimean Peninsula, far more advanced types of attacks on telecommunication nodes in Ukraine caused traffic to be rerouted to Russian-controlled servers. Analysis of this information gave them an advantage in understanding and anticipating Ukraine's moves in the following military operations.

In addition, hackers quite effectively interrupted select connections between Ukrainian activists and international resources in order to isolate the country from international platforms. After the "hot phase" began, Russian tactics became much more sophisticated, and military critical infrastructure also increasingly came under cyber attack. These assaults started with several script-kiddie attacks (unskilled hackers using programs developed by others) on the backbone military network, and gradually advanced to well-crafted whale phishing (targeted against wealthy, powerful or prominent people) and social engineering attacks (psychological manipulation to get the target to inadvertently reveal secure information) against high-ranking officers. Also worth mentioning were the unrelenting cyber espionage campaigns that rapidly became more sophisticated and complex. The Operation Armageddon campaign, started in 2013, was a cyber espionage effort to harvest sensitive data. The aforementioned NotPetya campaign contained a wide spectrum of tools and techniques, including substitution of financial software updates with malicious ones, ransom demands and data wiping. Given the situation in Ukraine, it is hard to overestimate the consequences of data leaks to date. These attacks are usually not directed at specific institutions — military, state agencies or private sector. Therefore, mitigation of impacts is the most efficient response for coordinated efforts on the governmental level.

In the military sphere, Ukrainian cyber defense units have also noticed increased persistence and sophistication in attacks (target-tailored exploits, multivector attacks, customized complex malware, zero-day attacks, etc.) against military targets as well as critical infrastructure objects. Mitigation of such threats requires not only comprehensive and multilayered defenses, but also cooperation among "defenders," including civilian services

Forensic experts gather evidence after a car bomb killed Col. Maksym Shapoval, a top Ukrainian military intelligence officer, the same day the NotPetya campaign was launched. REUTERS

A Ukrainian boy gazes at a photo of his father, a soldier killed in the war with Russian-backed separatists, at a memorial service in Kyiv in 2017. THE ASSOCIATED PRESS

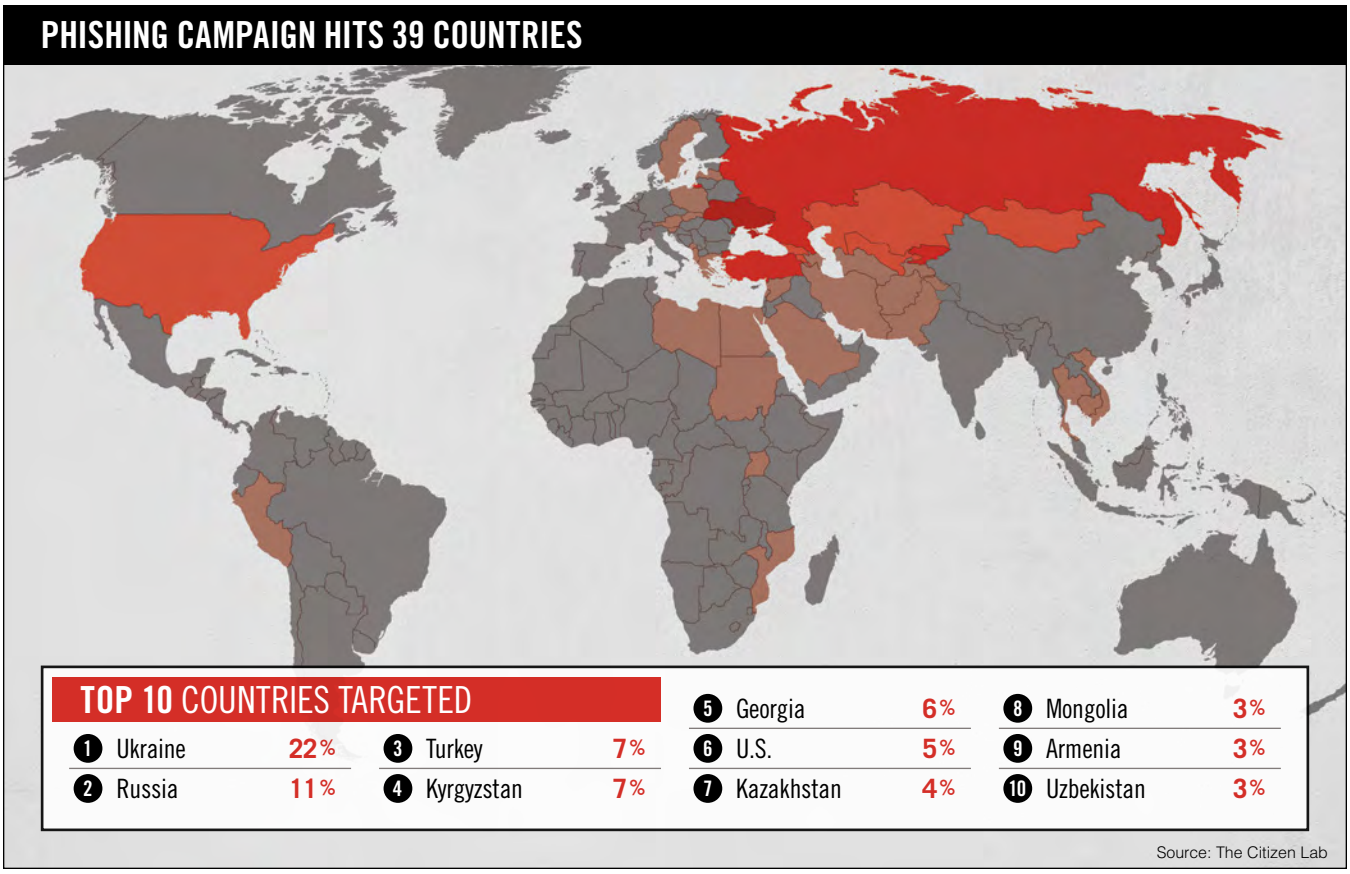
protecting critical infrastructure assets. To set up such cooperation venues at the state level, coordination and information-sharing systems should be reframed between government agencies and the private sector.

The past several years have seen an increase in the quantity and sophistication of cyber attacks against military and civilian critical infrastructure. This challenge is driving changes within the entire critical infrastructure cyber security system. For this purpose, coordination of cyber security by one state-level organization would be most efficient.

The changing threat

Analyses of cyber attacks against Ukrainian critical infrastructure reveal another interesting tendency. Increasingly, cyber attacks do not result in significant financial gains for the attackers. These attacks, most significantly, have a political resonance, social impact (increasing protest tendencies, manufacturing sympathy toward the aggressor), and degrade military capabilities (disruption of telecommunications, attempts to violate confidentiality in secure communications). This implies that the shift in attack vectors is achieving its desired results — namely, creating advantages that support a geopolitical narrative. Single hackers, usually involved in financial cyber operations, have not typically been able to orchestrate and conduct high-level cyber operations. For this reason, the conduct of cyber attacks against Ukraine's critical infrastructure is deemed to have evolved from individual hacktivists to organized, state-supported groups of highly experienced cyber experts, most likely with Russian support.

Over the past several years, advanced persistent threats (APTs) and state-supported groups of highly experienced cyber experts, capable of developing complex cyber weapons, began to appear. For instance, an FBI Joint Analysis Report on cyber attacks against the United States' 2016 elections identified two well-known Russian cyber-threat groups (APT 28 and APT 29) as the likely culprits. These groups have consistently focused on stealing intelligence for the Russian government. The majority of the cyber operations against Ukrainian critical infrastructure in the past few years were likewise most probably planned and



PER CONCORDIAM ILLUSTRATION

An extensive Russia-linked phishing campaign resulted in more than 200 stolen email accounts across 39 countries. Documents were used to manipulate data and plant disinformation.

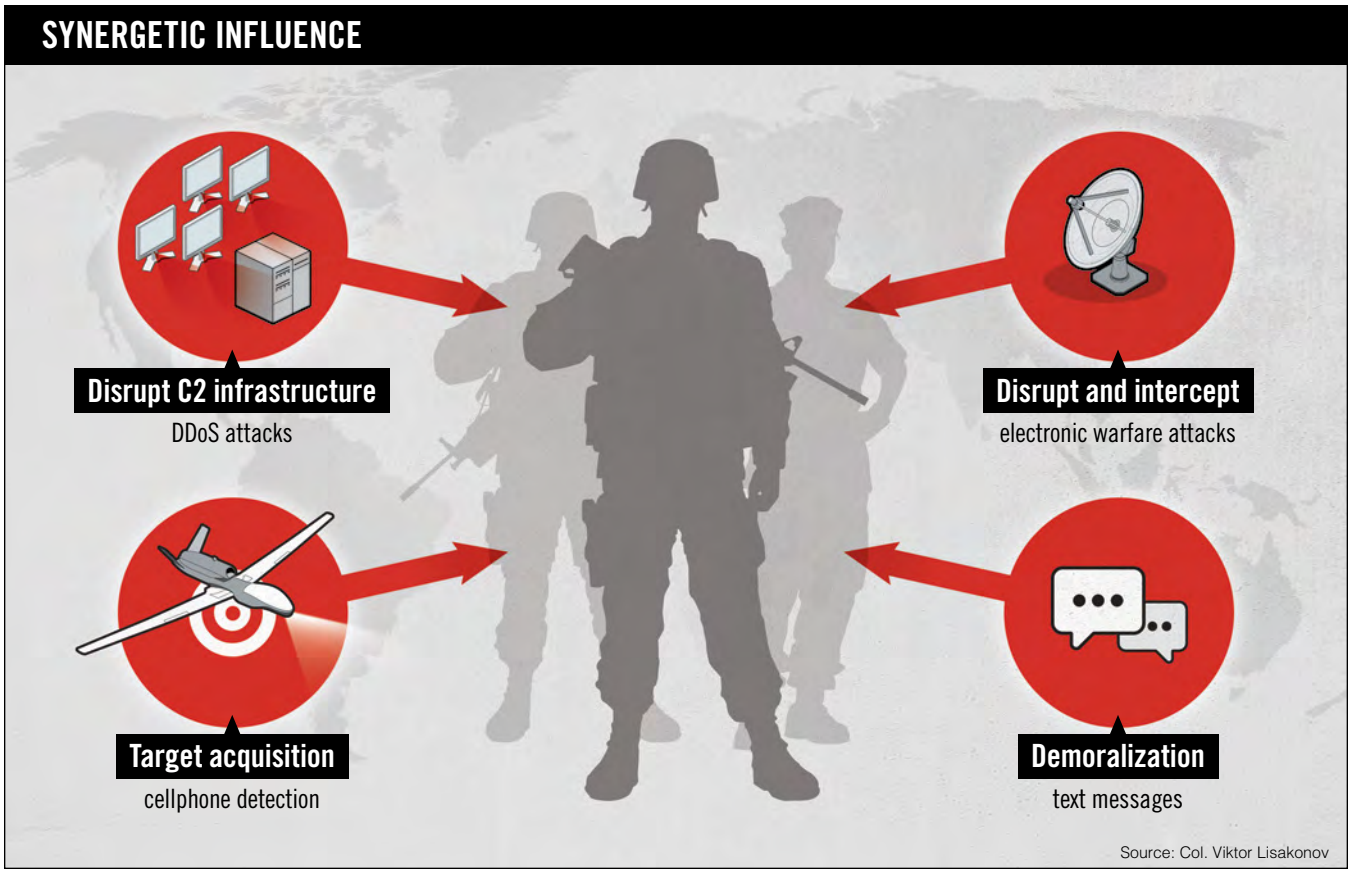
conducted by these groups. They have repeatedly targeted Ukrainian, European and U.S. government marks such as militaries, international organizations, think tanks, media and others closely linked to Russian geopolitical interests and priorities. The main goal of such groups is to create and maintain a geopolitical situation favorable to Russia that, together with stolen data, is used by Russian authorities during military operations or political negotiations.

The threat shift from individual hackers targeting financial institutions to state-supported groups of highly organized and professional technicians targeting critical infrastructure occurred in recent years. This shift has had a major impact on the orientation, priorities and capabilities of cyber security systems everywhere. Only a couple years ago, financial institutions or wealthy corporations were the most lucrative targets for highly experienced hackers. Today, military facilities and critical infrastructure are among the most frequently attacked targets.

Synergetic cyber attacks

Another great challenge worth mentioning is the synergetic use of different types of conflict tools. The synergetic approach includes attacks coordinated in time, place and targets to amplify the effects of each other. This approach is not new and Russia has already successfully employed it in Georgia. In his article "Cyberwar Case Study: Georgia 2008," David M. Hollis describes this as "the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains." However, the cyber domain and its borderless nature and anonymity bring another variable to the equation in light of Russian aggression against Ukraine. The annexation of Crimea began with a series of disinformation campaigns intended to create ambiguity and despondency, and delay Ukraine's responses. Huge armies of trolls created the image of strong support from the Crimean population for Russian action, and the same picture was broadcast on Russia-funded international TV channels, such as Russia Today and Sputnik, for consumption by foreign audiences. At the same time, to ensure information superiority, Russian special forces physically destroyed cable connections with the Ukrainian mainland and took over the internet exchange point.

During the Donbas invasion, Ukraine faced a much more complex and sophisticated assault. Prior to the hot phase of the conflict, Russian intelligence and cyber espionage campaigns created a very effective background for future combat operations against the Ukrainian Armed Forces. Having acquired this advantage, cyber attacks, electronic warfare, and psychological and informational operations were well-coordinated with strong kinetic attacks. This synergetic use of various assets and methods across



PER CONCORDIAM ILLUSTRATION

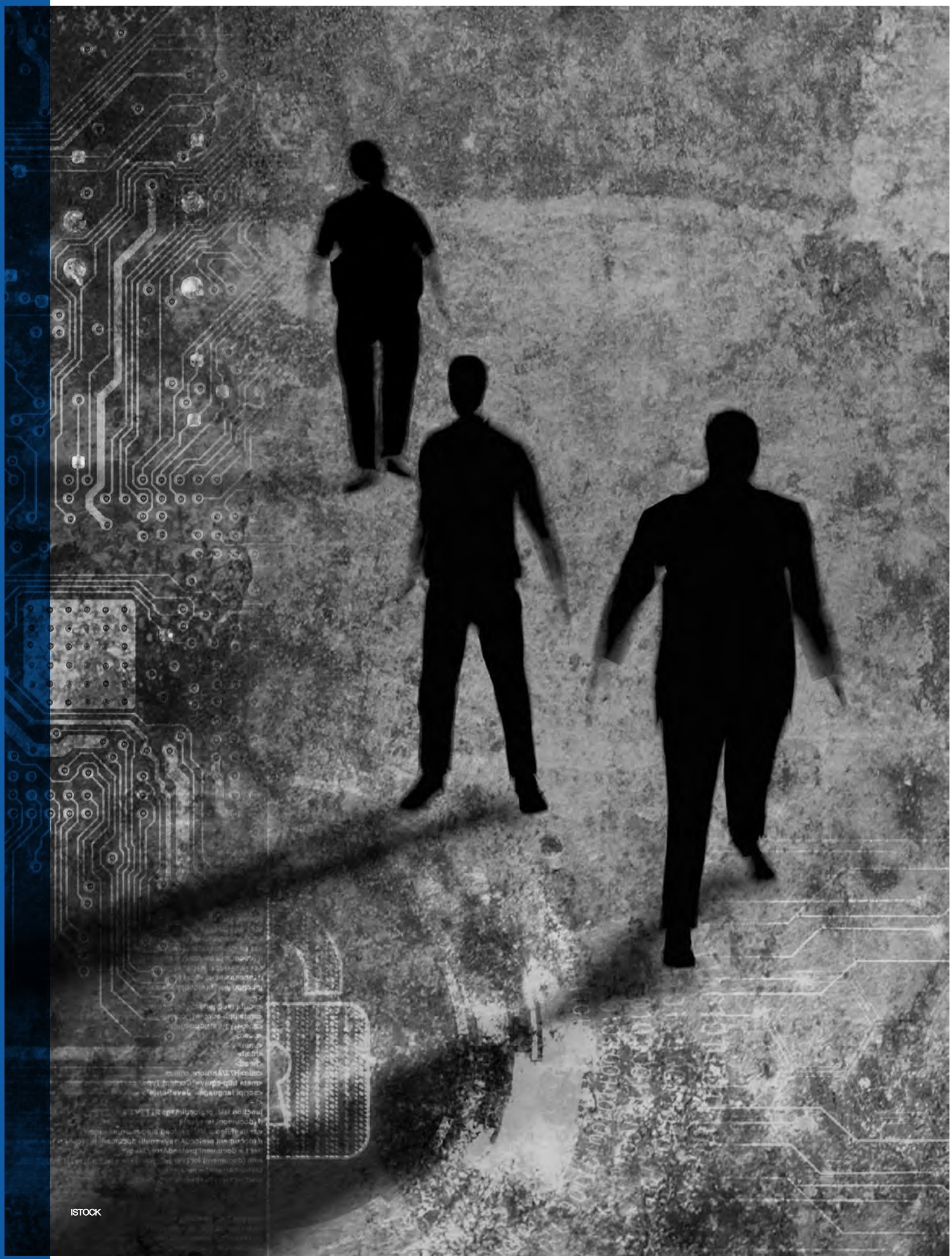
During major Russian operations, Ukrainian soldiers become the targets of complex, multidirectional influences that include electronic warfare and cyber psychological measures.

different domains enhanced the impact and frequently caused ambiguity among the attacked combat units. For instance, during Russia's Debaltseve offensive and the siege of the Donetsk airport, Russian specialists systematically broadcast demoralizing text messages to Ukrainian soldiers and their families. In addition, strong DDoS attacks were directed at command-and-control infrastructure, and tactical radio communications were interrupted by Russian electronic warfare. "During the 240-day siege of the Donetsk airport, the Russians were able to jam GPS, radios and radar signals. Their electronic intercept capabilities were so good that the Ukrainians' communications were crippled," Robert H. Scales wrote in his article, "Russia's Superior New Weapons." Traditional, powerful propaganda complemented the aforementioned. Social media were flooded with disinformation and panic messages. Hundreds of bots from troll factories and brainwashed pro-Russia individuals attacked the Ukrainian government and spread false stories about hundreds, or sometimes thousands of soldiers killed in action or captured.

This multilayered operation was coordinated in time, targets and objectives. A combination of cyber domain, electronic warfare, psychological and information operations, with simultaneous kinetic actions, damaged Ukrainian defense efforts. Taking into account the internal political situation in Ukraine and relations on the international stage, the synergetic use of such a wide spectrum of tools was a most effective strategy. But the most dangerous aspect of such an approach is that it is universal in scope and can be used to similar effect against any geopolitical opponent.

Conclusion

This author and his colleagues are directly involved in Ukrainian efforts to withstand such Russian hybrid aggression. The Gerasimov Doctrine entails the wide use of hybrid measures against an adversary to cause instability and internal conflict, just as it was executed against Ukraine. Objects of critical infrastructure are the most lucrative targets for such an approach. For the past decade, Russian offensive cyber capabilities have evolved from simple denial attacks to complex, multilayered operations that integrate simultaneous and coordinated usage of psychological, electronic and kinetic components, and financial and international pressure. A challenge in today's environment is that these offensive operations are neither fully understood by society and legislation, nor adequately addressed. This complex hybrid approach has potentially catastrophic impacts on critical infrastructure and the environment. Such attacks create disorganization, ambiguity and destabilization in society, which could create additional pressure on high-level decision-makers, leading to geopolitical benefits for the attacker. □



ISTOCK

RESILIENCE IS KEY

How to thwart known, and unknown, dangers

By **Lt. Col. Darko Galinec, Ph.D.**, Ministry of Defence of the Republic of Croatia | Photos by The Associated Press

Military terminology can migrate into nonmilitary contexts in the same fashion that military technology can migrate into civilian enterprises (for example, the Advanced Research Projects Agency Network later becoming the internet). In many cases, a migration of terminology is beneficial because it develops better specificity in discussions of technology operations. However, the utility of a term is reduced when its distinctive meaning is eroded or destroyed as part of the migration to a new context. Consider cyber security, which has been practiced in military circles for over a decade. But in recent years the term has appeared in a variety of contexts, many of which have little or no relationship to its original meaning. Its misuse obscures the significance of the practices that make cyber security a superset of information security, operational technology (OT) security, and information technology (IT) security practices related to digital assets.

Accurately defining cyber defense is equally important. In the context of a specific environment, cyber defenses analyze possible threats and help to devise and drive the strategies necessary to counter malicious attacks or threats. A range of activities are involved in cyber defenses when protecting the concerned entity and for responding to the threat landscape. These include: reducing the appeal of the environment to possible attackers; understanding the critical locations and sensitive information; enacting preventive controls to ensure attacks would be expensive; attack detection capability; and strengthening reaction and response capabilities.

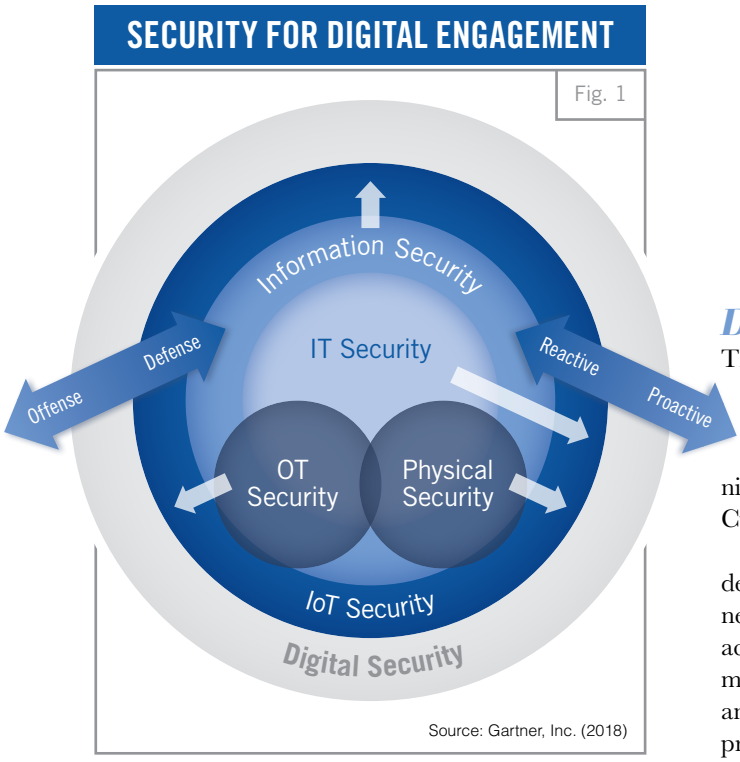
Defining cyber security

Cyber security is the governance, development, management and use of information security and OT security for achieving regulatory compliance, defending assets and compromising the assets of adversaries, as Daniel Dobrygowski wrote in a 2016 *World Economic Forum* article. According to experts, cyber security:

- Is a superset of the practices embodied in IT security, information security, OT security and offensive security (see Figure 1).
- Uses the tools and techniques of IT security, OT security and information security to minimize vulnerabilities, maintain system integrity, allow access only to approved users and defend assets.
- Includes the development and use of offensive IT- or OT-based attacks against adversaries.
- Supports information assurance objectives within a digital context but does not extend to analog media security (for example, paper documents).

However, cyber security is not:

- Merely a synonym for information security, OT security or IT security.
- The use of information security to defend an enterprise against crime.



- Cyber warfare (the consensus among experts is that cyber warfare refers to the use of cyber security capabilities in a warfare context, though this is a complex area and should not be confused with physical attacks against infrastructure, such as destruction of property and machinery, and information warfare, such as applying psychological operations through propaganda and misinformation techniques).
- Cyber terrorism (in a fashion similar to cyber warfare, cyber terrorism refers to the use of cyber security techniques as part of a terrorist campaign or activity).
- Cyber crime (this is merely a term for criminal attacks using IT infrastructure and is not related to cyber security).

Appropriate uses of cyber security:

- When responding to threat risk assessments, the department increased its cyber security investment to reduce vulnerabilities and increase capabilities for counterattacks against identified attackers (integration of IT security and offensive capabilities in a single program).
- Integrating IT and OT security programs within the cyber security team to enable more holistic responses to threats.
- When the "hacktivist" organization Anonymous employs a variety of cyber security techniques to forward its agenda (use of offensive capabilities).

Some inappropriate cyber security uses:

- To mitigate the theft of laptops, a store's cyber security plan calls for the use of whole-drive encryption (this describes a basic IT security action).
- A cyber security policy mandates the use of complex passwords for all computer-aided manufacturing systems on the factory floor (this describes a basic OT security requirement).

Defining cyber defense

There are no common definitions for cyber terms — they are understood to mean different things by different nations/organizations despite their prevalence in mainstream media and in national and international organizational statements, according to NATO's Cooperative Cyber Defence Centre of Excellence.

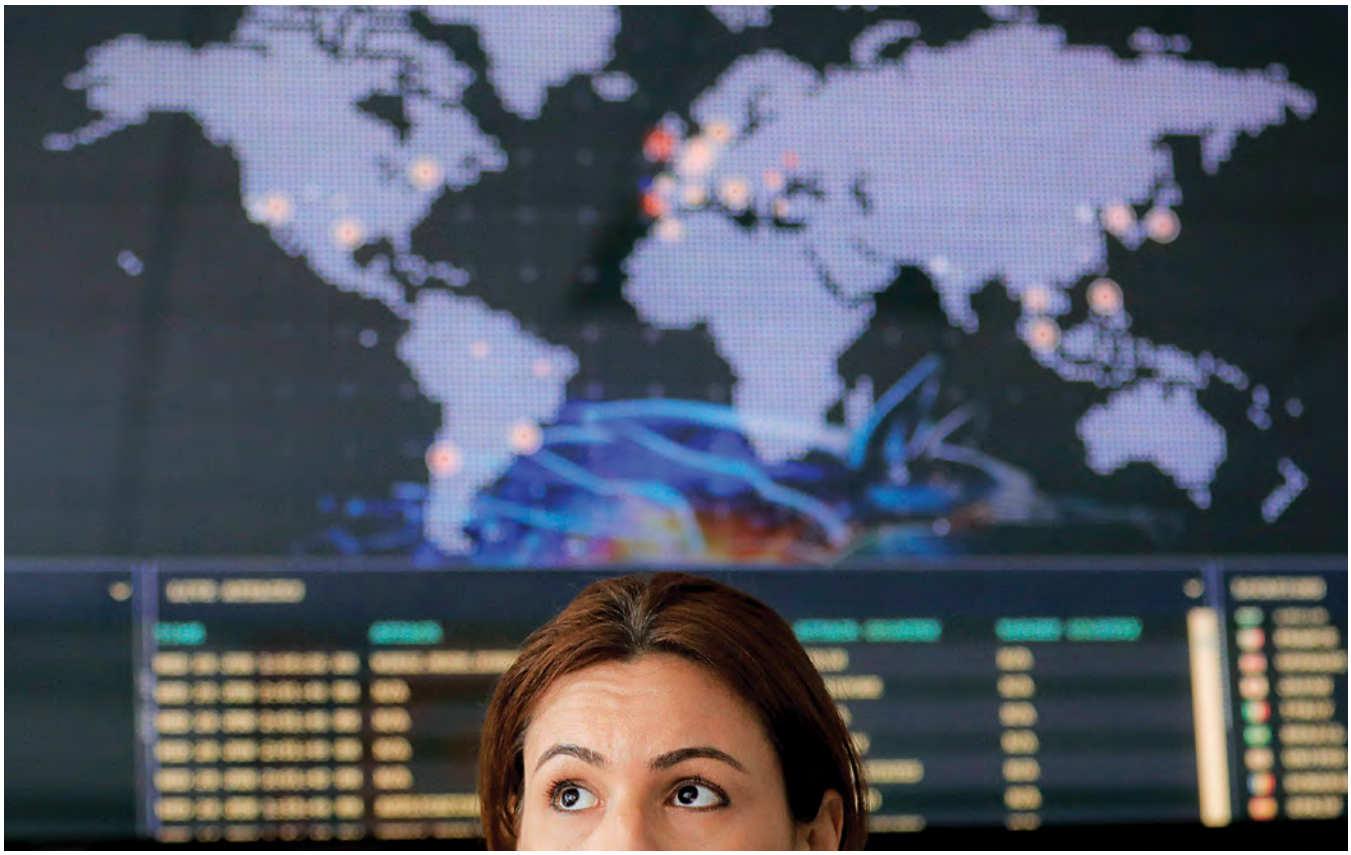
However, techopedia.com provides the following useful definition of cyber defense: "Cyber defense is a computer network defense mechanism which includes response to actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks. Cyber defense focuses on preventing, detecting and providing timely responses to attacks or threats so that no infrastructure or information is tampered with. With the growth in volume as well as complexity of cyber attacks, cyber defense is essential for most entities to protect sensitive information as well as to safeguard assets."

Cyber defense provides the much-needed assurance to run standard processes and activities free from worries about threats. It helps enhance security strategy utilizations and resources in the most effective fashion. Cyber defense also helps to improve the effectiveness of security resources and security expenses, especially in critical locations.

By recognizing the need to accelerate detection and response to malicious network actors, the United States Department of Defense has defined a new concept, Active Cyber Defense, as the department's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities.

While the cost of defending cyber structures — as well as the payoffs from successful attacks — is rising, the cost of launching an attack is simultaneously decreasing, according to infosecurity.net.

However, for today's world of asymmetric warfare and rapidly changing threats, the medical definition of "strategy" from Merriam-Webster's dictionary is more appropriate for addressing cyber security: "an adaptation or complex of adaptations (as of behavior, metabolism



A woman at the headquarters of the cyber security firm Bitdefender in Bucharest, Romania, sits in front a map showing real-time cyber attacks in 2017. Malicious ransom software can cripple computers globally.

or structure) that serves or appears to serve an important function in achieving evolutionary success."

The key to increasing cyber security is achieving lower levels of vulnerability. Although threat awareness is important, by reducing vulnerabilities all attacks are made more difficult, according to the technology research and advisory company Gartner Inc.

Risk management

Cyber security breaches, such as those at the online dating service Ashley Madison, the U.S. Office of Personnel Management, and J.P. Morgan Chase have demonstrated the real and present threat from cyber breaches. Adm. Mike Rogers, former director of the U.S. National Security Agency and former head of the U.S. Cyber Command, has been moved to state that "It's not about *if* you will be penetrated but *when*."

If there is insufficient visibility of cyber security status, organizations won't be able to manage cyber security risks and they will almost certainly suffer a breach. "Visibility of cyber security status" means having the complete picture, with measurements so that the following questions can be answered:

- What are the current measured levels of cyber security risk, across the enterprise, from multiple threats?
- Are these cyber security risks tolerable?
- If not, what is a justified and prioritized plan for managing these risks down to tolerable levels?
- Who is responsible and how urgent are the risks?

The ability to measure cyber security status is fundamental; if it cannot be measured, successful management becomes impossible. Security incident and event management (SIEM), as well as data analytics solutions, can provide valuable indications of actual or potential compromise on a network. However, these provide an incomplete picture: They are indicators of overall risk status, but not clear measurements of the risk status.

Similarly, threat intelligence services can identify data losses and provide valuable indications of actual or impending attacks, but again these are not measurements of risk status. The same can be said individually about outputs from compliance management, vulnerability management, penetration testing and audits.

Only through careful analysis of all relevant indicators and partial views can an overall risk-based measurement and visibility of the cyber security status be developed, according to Simon Marvell, a partner with Acuity Risk Management. When confidence in the cyber security risk measurements exists, it is possible to respond to events and make decisions quickly. To boost confidence:

- Identify risks that cannot be tolerated and have a clear and prioritized risk-based action plan for the control improvements necessary to reduce these risks to an acceptable level.

- Have a better understanding of the implications from threat intelligence or outputs from SIEM and data analytics, allowing faster, better-targeted responses.
- Develop risk-based justifications for investment in cyber security solutions and services.

However, with very high threat levels and high rates of change in both the threat and control landscapes, it is imperative for organizations to update their cyber security status (or posture) much more frequently, perhaps daily.

Whereas cyber security risk management previously might have been an annual process as part of planning and budgeting, it is now a critical, real-time facilitator in the battle against cyber breaches, according to Marvell. Cyber security breaches occur when people, processes, technology, or other components of the cyber security risk-management system are missing, inadequate or fail in some way. Therefore, it is necessary to understand the important components and how they interrelate.

A woman walks by cash machines that do not work in Kyiv, Ukraine, after a massive ransomware attack in 2017. The global onslaught hit Ukraine particularly hard.

For example, this doesn't mean that risk management systems need to hold details of every endpoint and the status of every vulnerability on the network, because there are other tools that will do that. But the risk-management system does need to know that all endpoints on the network have been (and are being) identified and that critical vulnerabilities are being addressed quickly.

In the end, success in cyber security is essentially the result of an effective risk-management process. However, this process faces significant challenges through the inherent complexity of systems, which have been developed with vulnerable components and protocols, and the growing sophistication of the attackers, who are often supported by well-resourced criminal organizations and nations.

Cyber resilience

Given the high level of uncertainty and high volume of events, it is essential to foster cyber resilience. Cyber resilience is the ability of a system, organization, mission or business process to anticipate, withstand, recover from and adapt its capabilities in the face of adversarial conditions, stresses or attacks on the cyber resources it needs to function. First recognized at the 2012 World Economic Forum in Davos, Switzerland, cyber resilience has become an area of growing importance for individuals, businesses and societies, and a concept that is gaining attention and usage, according to the academic paper, "Cyber Resilience — Fundamentals for a Definition."

Cyber resilience from an organizational perspective refers to the ability to continuously deliver the intended outcome despite adverse cyber events. The notion of "continuousness" infers that the ability to deliver the intended outcome should be retained even when regular delivery mechanisms have failed, whether during a crisis or after a security breach. The notion also denotes the ability to restore the regular delivery mechanisms after such events as well as the ability to continuously change or modify delivery mechanisms as needed in the face of changing risks. The intended outcome refers to that which the unit of analysis (e.g., the nation, organization or IT system) is intended to achieve, such as the goals of a business or business process, or the services delivered by an online service.

Cyber security is an inherently distributed problem that will continue to evolve at the speed of technology. According to the 11th Annual Global Information Security Survey, executives remain confident in the robustness of their security initiatives. Eighty-four percent of CEOs and 82 percent of CIOs contend their cyber security programs are effective, while 78 percent of chief information security officers express full confidence in their existing cyber security programs. However, with breaches on the rise, companies should focus on cyber resilience and not only on cyber security. The number of security incidents detected is rising significantly year

"It's not about *if* you will be penetrated but *when*," says Adm. Mike Rogers, former director of the U.S. National Security Agency and former head of the U.S. Cyber Command.

to year — from 2,989 reported in 2012 to 3,741 in 2013. Furthermore, the average losses per incident rose 23 percent over that period, and the number of organizations reporting losses of more than $10 million per incident increased 75 percent between 2012 and 2014, according to *Forbes* magazine.

Cyber security isn't going far enough, so cyber resilience must be taken into consideration. Once businesses accept that cyber attacks will be made against their organizations and will be successful, they can move to the next step: implementing a cyber resilience program. As defined in *Forbes*, such a program encompasses the ideas of defense and prevention, but goes on to emphasize response and resilience in moments of crisis.

Emerging risks

Today's security professionals battle threats from outside their organizations as well as those from their own employees. But what about threats that they already know exist? The next few years will see a variety of attacks as well as progress in the technologies and processes that prevent them.

Cyber security is no longer enough: There is a need for strategies of defense, prevention and response. The idea of resilience, in its most basic form, is an evaluation of what happens before, during and after a digitally networked system encounters a threat. Resilience should not be taken to be synonymous with "recovery." It is not event-specific; it accrues over the long term and should be included in overall business or organizational strategies. Resilience in the context of the ability of systems and organizations to withstand cyber events refers to the preparations that an organization has made with regard to threats and vulnerabilities, the defenses that have been developed, and the resources that must be available for mitigating a security failure. Normalization is key. Cyber risk should be viewed just like any other risk that an organization must contend with to fulfill its goals. Leaders of business and government need to think about resilience for two reasons: First, by doing so they avoid the catastrophic failure threatened by an all-or-nothing approach to cyber risks (such as preventing network entry as the only plan); and second, it ensures that the conversation encompasses more than only information technology or information security, according to Dobrygowski's article in the *World Economic Forum*.

The first point, that a long-term view and durability are key factors in ensuring cyber resilience, does not need further explanation. A plan that encompasses actions and outcomes before, during and after the emergence of a threat will generally be superior to a plan that only considers one incident at a time. The second point, that leaders must broaden the conversation, merits more attention. It is vital to economic and societal resilience that those engaged in cyber security think beyond information security to

The NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. According to the center, there are no common definitions for cyber terms.

overall network resilience to ensure existing risks — as well as new risks that may entail such things as artificial intelligence, the internet of things, or quantum computing — can effectively be dealt with. To ensure long-term cyber resilience, organizations must include in their strategic planning the ability to iterate based on evolving threats from rapidly evolving disruptive technologies.

By promoting an overall cyber-resilience approach, long-term strategy (including which technologies a business will implement over the next five, 10 or more years) is a continual strategic conversation involving both technology and strategic leaders within an organization. The cyber-resilience approach ensures greater readiness and less repetition — making it, on the whole, more efficient and more effective. Security, in contrast to resilience, can be seen as binary. Either something is secure or it isn't. As Dobrygowski writes, this is often relegated to a single, limited technical function, keeping unauthorized users out of a networked system.

While there are many broader definitions of cyber security, there is a difference between the access control of cyber security and the more strategic, long-term thinking cyber resilience should evoke. Additionally, since vulnerability in one area can compromise the entire network, resilience requires a conversation focused on systems rather than individual organizations. Therefore, resilience is best considered in the context of a public good or "commons." For this reason, partnerships are key. These can be between businesses as well as with regulators, prosecutors and policymakers.

Since cyber resilience is really a matter of risk management, there isn't a single point at which it begins or ends. Instead, it comes from building strategies and working to ensure that the risk-transfer mechanisms that work for more traditional threats are also brought to bear on new cyber threats. Responsibility for cyber resilience is a question of overall strategy rather than specific tactics. Being resilient requires those at the highest levels of a company, organization or government to recognize the importance of avoiding and mitigating risks. While cooperating to ensure greater cyber resilience must be everyone's responsibility, leaders who set the strategy for an organization are ultimately responsible and have increasingly been held accountable for including cyber resilience in organizational strategy, according to Dobrygowski.

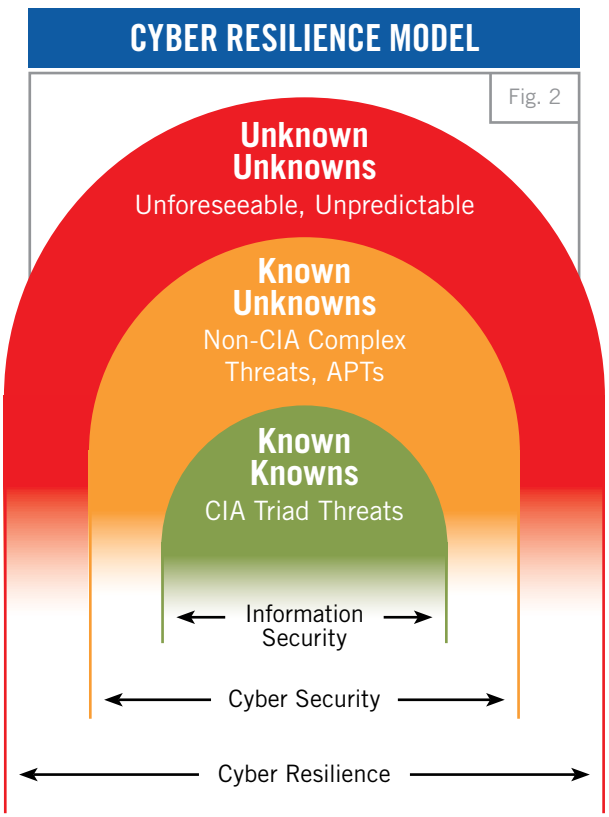
The real cyber security challenge is the unknown. Former U.S. Secretary of Defense Donald Rumsfeld gave this explanation during a news briefing in 2002: "There are known knowns. These are the things that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. These are things we don't know we don't know."

Combating known threats is an essential part of a cyber security strategy. It goes alongside advanced

capabilities to anticipate, capture and — ultimately — learn from unknown threats. Systems have different weak spots and different processes (challenges) and they each manage risk in different ways (solutions). In other words, to each security challenge (evaluated as known or unknown) is a corresponding solution to that challenge (evaluated as known or unknown). By incorporating values obtained during the system security assessment process into the model we get "known knowns" relating to information security, "known unknowns" relating to cyber security and "unknown unknowns" related to cyber resilience, according to the cyber security firm Exclusive Networks.

Example: There is a known crisis in the cyber security workforce — a massive shortfall in qualified and trained security professionals. There is also an unknown solution to this crisis. As *Federal Times* magazine reported, the broad and growing scope of the challenge requires a corresponding broadening of skill sets that are both known and unknown.

Finally, based on this author's best knowledge gained at the Program on Cyber Security Studies held in 2017 at the Marshall Center, a cyber resilience model structure and content is presented (Figure 2) consisting of information security (confidentiality, integrity and availability — CIA triad threats and responses to them, i.e, known knowns), cyber security (non-CIA complex threats, or advanced persistent threats (APTs), and corresponding responses to them, i.e, known unknowns) and cyber resilience (unforeseeable and unpredictable threats and responses to them — unknown unknowns).



Source: Lt. Col. Darko Galinec, Ph. D.

There are opportunities around those cyber security solutions that can take the fear out of unknown quantities, and make them known. But there continue to be significant opportunities around those protection measures that apply the universe of known cyber threat knowledge to keep the system continuously secure, according to the technology services company Exclusive Networks.

To cope with the growing challenges, which today are manifested as unknown unknowns, systems tend to enable personnel and develop new processes, organization and technology. Technologies are being developed which, unlike traditional approaches, have the ability to protect systems from serious threats by learning what is "normal" for the organization and its people and thereby spotting emerging anomalies. Unlike the traditional rules and signature-based approach, the technology can spot threats that could harm the organization and network that the traditional approaches would be unable to detect. It can deal with uncertainty and delivers adaptive protection for organizations from both insider threats and advanced cyber attacks.

Conclusion

Nowhere has technological development been more dynamic and comprehensive than in communication and information technology. The focus has always been on the rapid development and introduction of new services and products, while the security-related aspects usually have had little influence on the broad acceptance of new technologies.

The life cycles of modern-day information systems, from the process of planning, introduction and usage to their withdrawal from use, are very short, which often makes their systematic testing impossible and is most commonly applied as an exception in expressly prescribed cases.

Modern societies are deeply imbued with communication and information technology. People are nowadays connected using various technologies for the transmission of text, image and sound, including the growing internet of things. Deviations from the proper operation of these interconnected systems or their parts are no longer merely technical difficulties; they pose a danger with a global security impact. Modern societies counter them with a range of activities and measures collectively called cyber security.

Further investigation should be directed toward finding and enabling efficient and effective processes for agile (adaptable, aware, flexible and productive) cyber resilience of the security information system, so as to cope with unforeseeable and unpredictable events (unknown unknowns) in both internal and external environments of the system as a whole. Key roles related to that goal will have people and their performance at all levels within a system's hierarchy (cyber security combined with people-centric security) as key features of analysis. □

PUBLIC-PRIVATE PARTNERSHIPS

PER CONCORDIAM ILLUSTRATION

BUILDING A STRONG FOUNDATION FOR PROTECTING VITAL SERVICES

By **Agnieszka Wierzbicka**, Department of Cyber Security at the Polish Ministry of Digital Affairs

Over the past 10 years, information and communications technologies (ICTs) have become essential to the functioning of the economy as well as key drivers for development in all sectors. Governments, businesses, public and private organizations, and individuals have become dependent on the digital environment for their core activities.

Therefore, they all face a growing number of uncertainties. Cyber, digital and ICT hardware and software security threats and incidents have increased, leading to significant financial, privacy and reputational consequences, and in some cases even to physical damage. Digital security incidents can have far-reaching economic consequences for organizations. Examples include disruption of operations (denial-of-service attacks, disruption of information assurance and sabotage), direct financial loss of hundreds of billions of euros, lawsuits, reputational damage, the theft of intellectual property, technology and research, loss of competitiveness (theft of trade secrets), as well as loss of trust among citizens, customers, employees, shareholders and partners.

It is often said that information is power, and information being shared among partners is a key value of public-private partnerships (PPPs). This concept is particularly true in a world that moves at the speed of light — internet speed. Timely, accurate and expeditious sharing of cyber security-related information between organizations — in critical sectors, across sectors, nationally and internationally — is vital to effectively address the cyber security challenges of organizations. One of the key outputs of information sharing is the establishment of trust between people and organizations. Information sharing is an effective approach for managing collaborative cyber risk in a domain where the threat landscape is continuously changing. The sharing or exchange of information is increasingly encouraged by legislators and other stakeholders who recognize that reducing cyber security risks to government systems, critical infrastructures and enterprises increasingly depends on this form of proactive collaboration. However, the security benefits of sharing information must be achieved in a way that does not erode privacy or adversely impact individual freedoms and rights. Strong privacy and civil liberties protections are paramount if an information-sharing program is to be widely accepted and successful.

It is often said that information is power, and information being shared among partners is a key value of public-private partnerships. This concept is particularly true in a world that moves at the speed of light — internet speed.

No organization can address the full spectrum of its cyber security and cyber resilience on its own. Organizations are trending toward global interconnectedness and are consequently exposed to equally global cyber security threats. Collaboration with partners across organizational, functional, sectoral and national boundaries, and from small and medium enterprises up to multinational private enterprises and governments, is therefore required. This is essential to counter dynamic and multidisciplinary cyber security threats which may negatively impact an organization and its services. Moreover, in most cases critical infrastructure is privately owned and operated. The private sector holds considerable expertise in the development of internet policy, creation of cyber technology and defense against network intrusions.

It is essential to create an atmosphere in which both public and private parties show awareness of each other's need for discretion and act accordingly.

PPPs are used by public and private sector organizations to share information about incidents, vulnerabilities, threats, related strategic topics, operational methods and best practices. A number of countries, such as Germany, the Netherlands, the United Kingdom and the United States, have gained substantial experience with PPPs where they have brought together key stakeholders, including government, national agencies, regulators, information technology (IT) companies, IT security firms, business enterprises, private critical infrastructure and security researchers. This cooperation has evolved disparately, depending on the environment, culture and legal framework of a given country. Some of these PPPs have been legislatively or regulatorily mandated. Others have been developed by like-minded organizations of their own accord.

KEYS TO SUCCESS

Creating trust is vital for the success of any PPP because information shared within a PPP is often sensitive. It is essential to create an atmosphere in which both public and private parties show awareness of each other's need for discretion and act accordingly. Building trust is especially important when an initiative is based on voluntary information sharing and membership. In a trust-reliant PPP, it should be clear to all partners that the goal of cooperation is not to reveal stakeholder weaknesses or gaps in terms of cyber security. Effective PPPs create a climate of confidence and trust in order to share good and bad practices between applicable stakeholders, exchange experiences around events, discuss preparedness measures and even reactions from citizens or regulators in the broad subject area of information security. Trust is built among participants based on their contributions, collective actions and shared experiences.

There are various methods for building trust, such as informal meetings, small group meetings, transparency, teleconferences, networks of trust and reputation-based trust. Information sharing and analysis centers or information sharing and analysis organizations and the use of Traffic Light Protocol and of other standards establish rules on how information should be communicated. Within a framework of building trust there is significant value in creating an atmosphere of partnership from the outset. This can be achieved by reaching out to stakeholders early on, ideally at the "blank page" stage, and by an involvement of public and private sector partners at the priority, goal and objective phases of projects.

Continuous interaction between stakeholders is needed to foster cooperation. Trust is also built by establishing co-leadership of programs and consensus partnership decision-making. An effective PPP can be characterized by a clear set of rules that regulate the PPP framework, such as a memorandum of understanding, or in the case of larger membership, a (cyber) information-sharing agreement (or at a minimum, developed guidelines and etiquette to meet in a structured and useful way). The rules should prevent any conflict of interest and reduce ambiguity, indicate clear lines of responsibility and accountability, and set down achievable goals and establish incentives for partners. Another key to success is a clear common interest that establishes a basis for cooperation and creates a win-win situation. There has to be a balance between a private sector (which regards cyber security challenges as financial and a matter of reputation), and the public sector (where cyber security is viewed as a common public good).

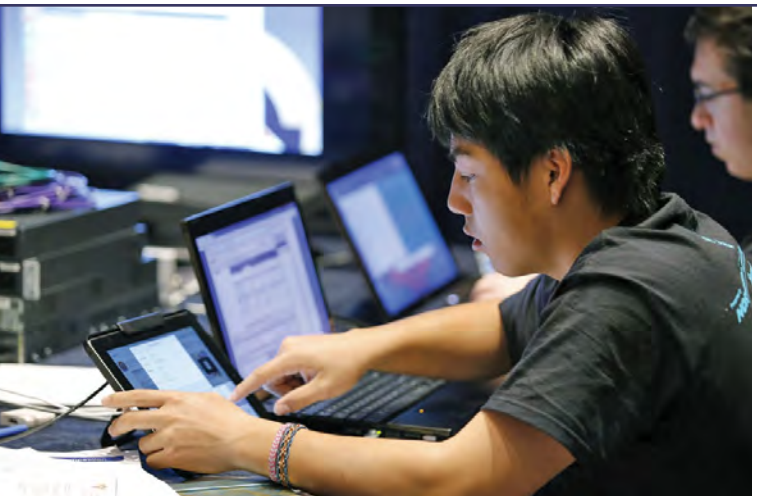
To avoid misunderstandings and mistakes, clarity about tensions and competing agendas is needed. If the partners' interests are not well-aligned,

Australian Foreign Minister Julie Bishop, center, visits the Telstra security operations center before speaking at Australia's inaugural International Cyber Engagement Strategy at the Telstra Customer Insight Centre in Sydney in October 2017.
EPA

governance by rules is advised. An awareness of each other's priorities, goals and limitations is necessary. This prevents conflict through misjudgment. Both public and private parties should know what drives each other and be able to evaluate whether objectives are still clear and that PPP activities align with these objectives. Collaboration is only feasible if both sides understand each other's objectives, their own mandate and standard operating procedures. Moreover, an organization's top management needs to have a clear view of the objectives and how they benefit the business objectives of that organization in areas such as the protection of shareholder interests.

Sharing of information is a significant benefit of a PPP. It is crucial that each partner provide equal value in-kind for information received within an appropriate time frame. This encourages each participant to cooperate and increases trust in the partnership. A secondary and equally important benefit is building individual personal networks. As mutual trust gradually increases, further information sharing is inspired. Energetic engagement by each participating organization helps build momentum by continuously adding value to all stakeholders. Senior-level commitment of public and private sector partners to the partnership process should be communicated to staff.

PPPs work best when the collaborating organizations operate at a similar maturity level. The maturity of the organization is displayed by its willingness to share sensitive cyber security-related information, the professionalism and experience of its cyber security staff and organization, and its ability to professionally and securely handle sensitive information received from other organizations. However, in some communities not all organizations are equally as capable or mature as others. Larger



The cyber defense competition CyberCenturion, a partnership of Northrop Grumman, the U.S. CyberPatriot Nation Youth Cyber Education Program and Cyber Security Challenge U.K., helps address the cyber skills gap.

THE ASSOCIATED PRESS/ GLOBE NEWSWIRE

organizations still may benefit from protecting and investing in information sharing with smaller organizations because this can positively impact a sector's image. Organizations have different backgrounds and ways of operating, especially in an international context. They have their own culture, history, language, judicial system, political and ethical differences, as well as experiences, norms, procedures, processes and practices. Some are public and some private, and some are more open to cooperating than others.

Language differences can stem not only from translation between different languages, but also from different vocabulary or technical terms (sector-specific slang). Insufficient attention to such differences on the edges of interaction between people, technology and processes may hamper collaboration and information sharing. Involving individuals who can cross cultural barriers as facilitators may help to stimulate the information flow between diverse communities. Moreover, organizations should not be pressed to share information against their wishes. If required to do so, their reluctance may be demonstrated negatively, for example, by overloading the recipient with low-value information. However, in some instances such as cases of national security and public safety, there may be a need for mandatory incident reporting. An ongoing debate rages between mandatory and voluntary information sharing. This is not an exhaustive list of key factors for the establishment or maintenance of successful PPPs, but they are characteristics worthy of consideration that have been identified by numerous research studies.

CHALLENGES

There are many challenges for PPPs that create obstacles to information sharing. It is sometimes contrary to private-sector commercial interests to report vulnerabilities, particularly if understanding and rectifying a problem before competitors become aware of it could offer a market edge. The public sector also encounters limitations to sharing information. Classified and sensitive information, as well as trade secrets, cannot be shared with individuals who do not have adequate security clearance. Even those working in the private sector who do have security clearance can often do nothing with classified information because of laws and regulations. Further, the high expectation that threat information shared from the public to the private sector will be accurate leads to extensive and stringent review and revision processes that delay the release of time-critical information. High public-sector staff turnover often hinders effectiveness, especially regarding trust issues. Hesitation to share information may also stem from the fact that passive and perhaps noncontributing members of PPPs are not penalized or because the conditions to join some PPPs are rather informal. A lack of respect for the confidentiality of information or for established rules of cooperation to which stakeholders have agreed could be even more counterproductive for a PPP. An efficient information exchange between organizations from different countries is also hindered by different laws and local regulations imposing data localization requirements and information storage restrictions, as well as information secrecy and nondisclosure rules.

Certain countries or sectors presume information sharing on cyber incidents may ultimately be interpreted through local or European regulations as anti-competitive behavior and, hence, likely to infringe on competition rules. Furthermore, law enforcement and other public officials may have multiple conflicting tasks and role ambiguity. Sharing detailed threat information to enhance common situational awareness may also, under certain legal frameworks, oblige a law enforcement official to change hats and use that information for investigative purposes. As a result, the source of the information may be leaked in the courts or may damage the reputation of the affected organization(s). National laws and regulations on personal data protection are additional barriers in the information-sharing process. For example, national laws that consider IP addresses as personal data do not allow organizations to exchange this type of information, even if it could be helpful to other companies.

RECOMMENDATIONS:

- **Ensure whole-of-society community involvement.** A PPP should be informed by knowledge of the partners most appropriate to accomplish its goals. Both public and private entities have vested (though varying) interests in cyber security and must be engaged. Because leadership support at the highest levels is key to success, public-sector engagement should include representatives from key ministries for cyber security. The engagement of state, local and territorial government entities is also important to ensure the security of critical digital infrastructure at the regional and local levels. International governments must be engaged too, either through inter-governmental channels or directly through PPPs, to ensure the interoperability of both technical and policy solutions. Finally, the sphere of appropriate private-sector partners includes both industry and the nonprofit community, with the latter encompassing academia and advocates for privacy and civil liberties. For example, the involvement of nonprofit organizations focused on internet governance is imperative to achieving policy coordination, while those focused on technological advancement are vital to fostering research and development in cyber security — as are their academic counterparts in either

European Commission Vice President Andrus Ansip, from left, European Union Security Union Commissioner Julian King and EU Digital Economy and Society Commissioner Mariya Gabriel speak about cyber security in Brussels. REUTERS

arena. It is equally important that private-sector partners include industry entities of varying size, from the largest corporations to small startups. Further, while the support of senior leaders from each sector is vital, it is equally important that partnerships extend to the tactical levels within partner organizations to ensure that the most nuanced engagement occurs between experts at any rank.

Building together the cyber security ecosystem fosters national and business goals as it provides market development and public safety.

- **Establish clarity regarding tensions and competing agendas.**
  Government stakeholders appear to approach cyber security as a matter of national security. They require information and expertise from private-sector entities to secure cyberspace effectively, and thus consider partnerships a public good. In contrast, their private-sector counterparts appear to view cyber security as a necessary expense in order to safeguard investments in intellectual property and other assets. Partnership with the public sector is of interest only to the extent that it furthers the goal of maximizing profit. By clearly establishing an end goal, partners can more easily overcome cultural differences, achieving success even while working toward it in very different manners.

- **Build trust that corresponds to a mutual belief in positive gains for both partners.**
  Trust is essential to all successful relationships and can be built only over time and, primarily, through personal relationships. PPPs should implement policies which maintain continuity of membership, backed by incentives. Having the right people in the partnership is another way to develop trust. Members that bring value that cannot be gained elsewhere will increase the motivation to build trusted relationships. In addition, trust must be built both ways. This means a recipient of information will not abuse it nor cause harm to the source, but must also trust in the source to be confident that the information is accurate and not misleading. That is why PPPs should adopt information distribution policies such as the Traffic Light Protocol to give the source confidence that the information will only be used as agreed. Moreover, in some cases it is necessary to include nondisclosure agreements, and arrangements for sharing sensitive information.

- **Develop incentives on behalf of the public enterprise.**
  As much as trust-building is vital in developing true partnerships, Rachel Nyswander Thomas and Larry Clinton stress in their respective studies for the Center for Strategic and International Studies and in the *Journal of Strategic Security* that incentives must also be properly aligned to reward each sector for their engagement. An incentive-based approach is best accomplished by tying incentives to results rather than activities. Incentives may include reduced risk exposure through better security and resilience; cost savings from sharing the labor to solve a critical problem; access to privileged information from government; access to knowledge not available elsewhere; opportunity to avoid inappropriate regulation; opportunities to contribute to strategic direction and national policies; technical knowledge; intelligence, research and analysis; leveraging the skills, experience and organizational positions of other members; and revoking membership for not contributing or attending meetings.

- **Establish a legal/regulatory framework.**
  The proliferation over the past decade of PPPs focused on securing cyberspace suggests that legislation is not necessary for public and private entities to work with one another. However, legislation could help create a regulatory environment more conducive to voluntary partnerships such as those in the financial or telecommunications sectors. Measures clarifying the authority various public institutions have to aid the private sector in the case of cyber intrusions would enable such public institutions to respond to requests better and in a timely manner, making private entities more likely to see value in partnership. Such rules should prevent any conflict of interest and reduce ambiguity.

- **Design a bottom-up approach.**
  A partnership driven primarily by a need for accountability will require more rigid infrastructure (and perhaps a contractual network of sorts), whereas a partnership valuing flexibility will be better suited by a looser framework. Given that cyber security is a matter of national security, it

Germany's telecommunications giant Deutsche Telekom AG opened Europe's largest integrated Cyber Defense and Security Operation Center in Bonn in October 2017.
REUTERS

might seem logical to value accountability above flexibility in the design of a related PPP. However, the fast-evolving nature of cyber threats, and the need for rapid technological advancement to address such challenges, makes flexibility extremely important in a cyber security PPP. This does not preclude regulatory mechanisms to encourage accountability, but the structure of the PPP itself must be flexible enough to meet its objectives as cyberspace evolves.

- Create a sound and sustainable financial package (U.K. case).
  Government can add value and reduce economic barriers to PPP participation by covering the costs of administration and venue.

- Maximize transparency.
  Clearly inform the participants of the relevance and real added-value of the PPP and be transparent regarding the rules and practices followed.

- Appropriate risk allocation and risk sharing.
  Cyber security-related issues need to be part of the permanent risk-management cycle of an organization.

THE WAY FORWARD

Public-private partnerships remain a vital and effective tool for achieving national and business cyber security goals. Common efforts to prevent, protect against, mitigate and recover from attacks are the best way to secure cyberspace. But to shift the balance in favor of resilience and strong protection, while at the same time allowing innovation, requires resources focused on research and development, technical standard setting, national and international policy development, and the building of human capital. Building together the cyber security ecosystem fosters national and business goals as it provides market development and public safety. □

The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of the Polish government, the Ministry of Digital Affairs or any of its agencies.

REDUCING RISK

THE CZECH REPUBLIC RESPONDS TO GROWING THREATS

By Veronika Netolická and Martin Konečný

PHOTOS BY REUTERS

Damage to the Czech Republic's critical information infrastructure (CII) has the potential to impact national security by affecting basic living conditions, people's health or the state's economy. The country's National Cyber Security Strategy for 2015-2020, its Security Information Service's 2015 Annual Report, and the National Security Audit all identify fundamental threats in this area. As revealed in these documents, cyber espionage is a serious CII threat. However, it is not the only threat. Unverified and unsecured hardware and software supply chains, ransomware and cyber terrorism also pose significant dangers.

CYBER ESPIONAGE

Cyber espionage seeks to obtain strategically sensitive or important information from individuals or organizations by using or targeting a means of communication. Cyber spies can gain political, economic or military advantage, posing a considerable threat to national security.

According to the Czech Republic's Security Information Service's 2015 report, the country faced major cyber espionage threats from Russia and China. That year a Russian cyber espionage campaign targeted two Czech ministries. Those two countries are not new to cyber espionage and their campaigns also target CII. In this area, for example, advanced nanotechnology research in the Czech Republic — a field for which the country is recognized — could become a target. The allure of obtaining crucial information, whether technological or political, makes such research a valuable target.

What makes cyber espionage especially dangerous is the low detection risk. In many cases, ongoing campaigns are detected months or even years after being launched. States must actively defend themselves against such campaigns. Also, the data obtained may be used not only for espionage purposes, but sometimes for extortion or further dissemination. Cyber espionage can also function as the backbone of more sophisticated cyber attacks. Retrieval of classified information can be targeted via the login details and personal data of prominent people who can be exploited. As digitalization increases and the volume of CII entities grows, cyber espionage campaigns are becoming more common and intense.

SUPPLY CHAIN SECURITY

According to the Security Information Service's annual report from 2014, supply chain security breaches can be used to threaten national security. For example, by using vulnerable hardware devices, the computer systems in CII could be penetrated. In this case, security risks arise from states' heavy dependence on hardware and software purchased from external suppliers, which might in turn be a source of cyber espionage.

As a case example, in 2010 the U.S. Navy purchased thousands of microchips from China for use in everything from missiles to transponders to rocket launchers. These microchips, however, contained a "back door" that allowed for remote shutdown of systems using them. In 2013, the U.S. Congress officially identified China's activities as a cyber threat. The U.S. banned the purchase of government supplies from Chinese companies, and it was also recommended that American private companies limit purchases of Chinese software. Because microchips can be programmed to actively interfere with a system, it is important to verify the hardware and software being used. In the Czech Republic, as in many other countries, suspicions revolve around Chinese vendors such as Huawei or ZTE.

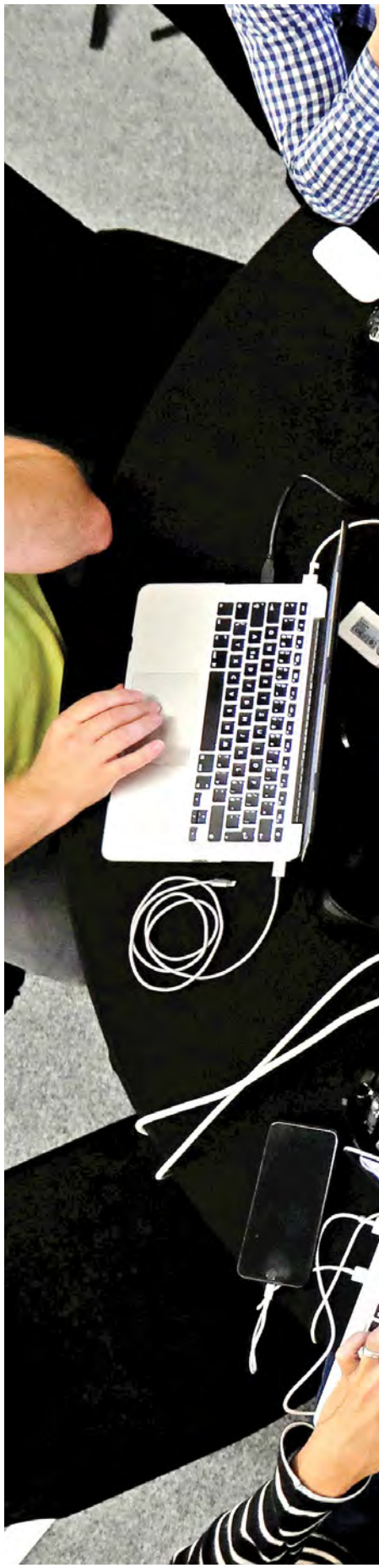
RANSOMWARE

But the damage may not be restricted to hardware. It may also involve the use of malicious programs such as ransomware, which blocks computer systems or encrypts recorded data and keeps it locked until a ransom is paid. Such attacks also pose a significant threat to CII.

The biggest ransomwares (WannaCry, Petya) targeting the infrastructure of states didn't directly affect the Czech Republic. But there is no guarantee that won't change because the criminal use of ransomware is so profitable. The best protection against ransomware is, at a minimum, regular backup of important documents to a device independent of the computer on which the data resides. After a ransomware attack, in most cases — even when the ransom is paid — the data is not returned. Even if it were, the confidentiality of the data is compromised.

CYBER TERRORISM

Cyber terrorism is a relatively recent phenomenon, and there is no consensus within the security community on defining the term. Recent attacks do not match the characteristics of conventional terrorism. According to the Czech National Security Audit from 2015, security is less threatened by a cyber terrorist attack than by a cyber espionage campaign. Though the Czech Republic might not currently be at a high risk for cyber terrorism, the risks can be expected to rise in the future. However, a discussion about this phenomenon should not be neglected now because the potential impact on CII could be catastrophic.



Photographers work on computers at an election headquarters in Prague, Czech Republic, in 2017. A solid legal foundation is key to cyber security.

LEGISLATION

A comprehensive legal framework provides a solid foundation for the protection of CII. The Act on Cyber Security, a cornerstone of Czech cyber legislation, became law on January 1, 2015, and was amended two years later.

The amended act regulates the following entities:

- Critical information infrastructure
- Operators of essential services (OES) (per the network and information security (NIS) directive)
- Important information systems (IIS) of public authorities
- Digital service providers (DSP) (per the NIS directive)
- Internet service providers (ISP)
- Significant network (or significant ISP) with secure network connection abroad or to CII

Implementing legal regulations related to the act cover:

- Cyber security requirements
- Determination criteria of OES
- Determination criteria of IIS
- Governmental cloud security (defining security requirements for public authorities)

The government institution responsible for cyber security is the National Cyber and Information Security

A man monitors a protest rally in front of Prague Castle in the Czech Republic in 2017. Attacks on critical information and communications systems threaten national security.

Agency, which operates the National Cyber Security Centre (NCSC). The NCSC has two integral parts — the government CERT (computer emergency readiness team) and Cyber Security Policies Department. According to the Act on Cyber Security, an additional CERT is responsible for cyber security for the rest of the country — the national CERT. The government CERT protects CII, OES and IIS and handles cyber security incidents; the remaining regulated entities (ISPs, significant networks and DSPs) fall under the national CERT.

Another legislative piece related to CII is the Crisis Act, which defines the determination process for CII elements. The Crisis Act is within the competency of the Ministry of Interior. The NCSC cooperates with the Ministry of Interior on determination of CIIs. Therefore, the role of the NCSC, alongside incident handling support, is to provide support with cyber security controls implementation, penetration testing, the conduct of cyber security exercises and support for cyber security education.

The NCSC is also responsible for performing inspections (cyber security audits) of all involved entities.

REDUCING RISKS

Considering the possible impact of cyber security incidents on national security, CII protection and OES efforts are top priorities for the Czech Republic. Accordingly, requirements on cyber security controls for these types of regulated entities are relevant to their importance.

The Czech approach to mitigating cyber risks is built upon a risk-based approach. In other words, it is based on the ability of companies/institutions to manage potential risks against their own systems. The aim is to decrease risks that could cause an unfavorable impact at the state level as well. The CII and OES must fulfill security requirements, defined by law, to mitigate risks. These are described in the Order on Cyber Security Requirements, which covers the following organizational and technical areas:

- Information security management systems
- Asset and risk management
- Organizational security
- Security policy and documentation
- Supply chain management
- Personal security
- Operation and communication management
- Change management
- Access management
- System acquisition, development and maintenance
- Cyber security event and incident management
- Continuity management
- Physical security
- Network security
- Identity management
- Malicious code protection
- Log management
- IDS/IPS
- Security information and event management
- Application security
- Cryptography
- Industrial cyber security and supervisory control and data acquisition
- Security
- Digital services security
- Audit

The current amended version of the Order on Cyber Security Requirements was drafted in cooperation with a team of cyber security experts from the private and public sectors. The team was composed of representatives of regulated entities and cyber security experts. Recommendations from the European Union and the European Union Agency for Network and Information Security were included.

As was already mentioned, the NCSC provides support for practical application of security requirements defined by this order. In 2017, the NCSC started a project of security audits for the most important government institutions. The aim is to recommend risk mitigation and to improve cyber security and cyber defense. This project is carried out annually.

LESSONS LEARNED

Although the legislative framework and safeguards of the Czech Republic have created a solid foundation for CII protection, cyber security cannot be maximized without a willingness on the part of CII entities to protect their own systems. Therefore, the Czech Republic aims to create an environment in which CII operators must implement basic safeguards to strengthen the security of their systems.

The state plays an important role here, acting more as a partner than a sanctioning authority. Building trust between CII operators and the state is the starting point. For example, consultations are now held between state experts and CII entities about upcoming laws. In 2017, a nontraditional stand was taken on the drafting of the Order on Cyber Security Requirements, and professionals from the public can provide content feedback and suggestions before the legislative process begins.

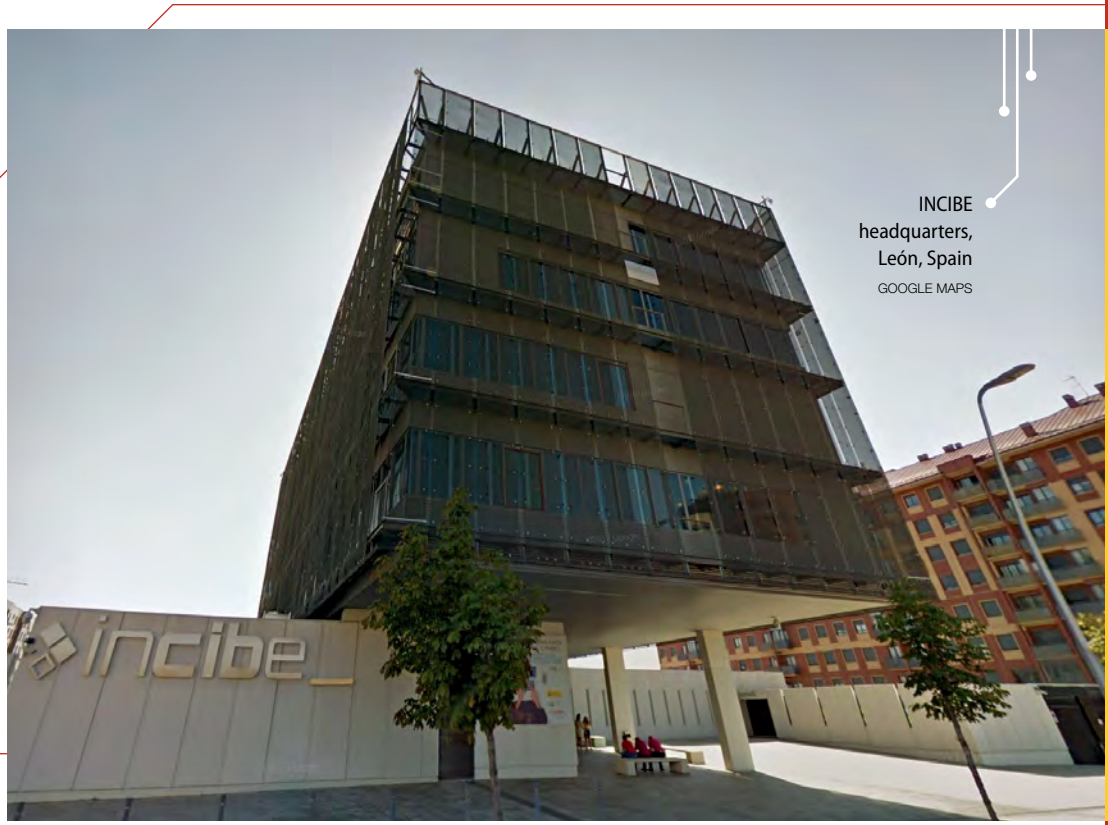
An approach based on trust opens up possibilities for sharing information. Effective information sharing will allow an understanding of incoming threats in greater detail and will contribute to introducing adequate measures, which, if implemented, can prevent future cyber incidents. Each state must realize that reducing risks in cyberspace is a never-ending, comprehensive process, and that the state should become involved and remain dynamic in cyber activities. □

SPAIN'S DIGITAL DEFENSES

Applying Innovative Models to Protect Critical Infrastructure

By **Alberto Hernández**, CEO, National Cybersecurity Institute of Spain (INCIBE)

PER CONCORDIAM ILLUSTRATION



INCIBE headquarters, León, Spain
GOOGLE MAPS

There have been a number of large-scale cyber attacks on critical services and critical infrastructure that have been widely covered in the media. But there have also been attacks with similar impacts that have gone largely unnoticed. These attacks will increase as the connectivity of industrial control systems, communications networks and internet-of-things devices continue to grow. This connectivity has many advantages in operation and management, but introduces new threats related to the internet, or cyberspace, domain. Cyberspace's global scope, low cost of access, anonymity, asymmetry, and its operational time measured in milliseconds are characteristics that hasten the rapid evolution of these new threats.

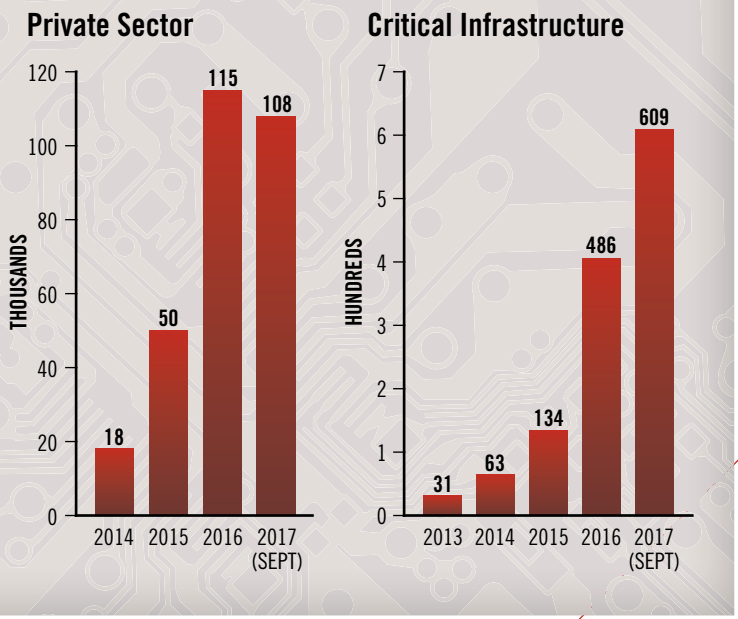
Attacks can vary in impact. In 2000, more than 2 million liters of untreated water was dumped into rivers and parks in Maroochy, Australia, as a result of several remote cyber attacks by a disgruntled worker. In 2008 in Lodz, Poland, four trains were derailed and several people were injured because a 14-year-old turned his television remote control into a device able to change the switch rails of the tracks. In June 2010, Stuxnet was discovered. This was the first known malware designed to spy and reprogram industrial control systems affecting critical infrastructure such as nuclear power plants. More recently, in 2015 in Ukraine, several power outages in the electrical distribution network left 1.5 million people without electricity for several hours. These cyber attacks show that the threats to essential services and critical infrastructure are real and that it is necessary to define and develop strategies to reduce and manage the associated risks.

In Spain, the number of cyber security incidents affecting citizens and the private sector is increasing, from about 18,000 in 2014 to 50,000 in 2015, and from over 115,000 in 2016 to 108,000 through September 2017. Regarding critical infrastructure, the number of incidents has also grown during the past four years, from 31 in 2013 to 63 in 2014, 134 in 2015, 486 in 2016, and to 609 through September 2017. Response to these incidents is managed by the Security and Industry Computer Emergency Readiness Team (CERTSI) operated by the National Cybersecurity Institute of Spain (INCIBE) and the National Centre for Critical Infrastructure Protection (CNPIC). This growth in the number of managed cyber security incidents may be due to three causes: an increase in cyber attacks, the improvement of CERTSI detection capabilities, and greater trust between CERTSI and strategic operators. This is evidence of the need to establish a strategy for critical infrastructure protection that can help organizations improve cyber security.

INCIBE's Strategy

In 2007, the Spanish Ministry of the Interior created CNPIC with the objective of protecting national critical infrastructure, including in the cybernetic domain. With the approval that year of a law protecting critical infrastructure, Spain

CYBER SECURITY INCIDENTS IN SPAIN



Source: CERTSI

established the appropriate strategies and structures to direct and coordinate the actions of the different public agencies involved in protecting critical infrastructure, with cyber security considered a key factor in all sectors.

To facilitate regulatory compliance and implement the most recognized practices for the improvement of cyber security, INCIBE, in collaboration with CNPIC, developed a comprehensive and specific strategy for critical infrastructure covering aspects such as prevention, protection and reaction in the event of a security incident. This strategy includes the following lines of action:

A. **ENSI:** The national cyber security framework is known as the National Scheme on Industrial Security (ENSI). It features common methodologies and tools for improving capabilities, minimizing the risks to which essential services are exposed, and establishing methodologies and measures to mitigate the risks applicable to industrial organizations.

High-voltage power lines are repaired near Slavyansk, Ukraine. In 2015, cyber attacks on the power distribution network left 1.5 million people without electricity.

AFP/GETTY IMAGES

ENSI is composed of a general policy and three units: cyber resilience improvement measures (IMC), a value chain cyber security capability building model (C4V), and lightweight risk management in integral security (ARLI-SI).

- **IMC:** The IMC model defines a set of indicators for improving cyber resilience as an instrument to diagnose and measure the ability to withstand and overcome disasters and disturbances emanating from the digital field.

  The question at this point is not whether an organization and its systems, including those related to essential services, are going to be attacked, but whether it will be sufficiently prepared to resist it, prevent essential services from being interrupted, and be able to recover in the briefest time possible. In short, is the organization cyber resilient?

  In the cyber world, the concept of cyber resilience rests on the need for organizations to be capable and ready to respond quickly to attacks, keeping the services they provide free of interruption while strengthening their capacity to identify, detect, prevent, contain, recover from, and cooperate and continuously improve against cyber threats.

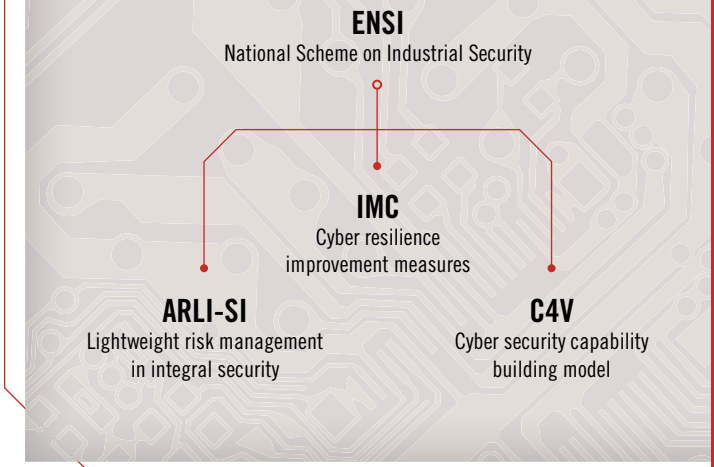
  INCIBE developed this comprehensive framework for measuring an organization's cyber-resilience indicators after conducting an international review of the National Cyber-Security Strategies, which are the main cyber security standards, metrics and indicators. The IMC model includes 46 metrics covering four main goals of cyber resilience: anticipate, resist, recover and evolve.

IMC GOALS

- **ARLI-SI:** The ARLI-SI methodology is a lightweight, risk-management methodology that is intended as a practical and simple risk-assessment model. It is centered on industrial control systems as the starting point and is a cornerstone of the safety improvement process.

  After a normal audit process, critical operators are provided with an initial diagnosis of the security of their systems. However, it is essential that they get additional information about steps needed to improve security and what is considered an adequate cyber security level.

SPAIN'S NATIONAL SECURITY FRAMEWORK



- **C4V:** INCIBE developed the C4V to give operators an understanding of the degree of maturity and robustness of the protection measures implemented in critical infrastructure systems. The C4V pays special attention to the dependence of essential services and to risk management in the information and communication technology supply chain.

  One advantage of this model is that, in cases where third-party service providers affect the capacity level, the organization responsible for the service must establish mechanisms to ensure that such third parties meet capability requirements. The third parties should also have monitoring procedures to ensure that this level is maintained throughout the service life cycle.

B. The Spanish platform for sharing cyber security threats, known as the ICARO system, is a tool to help identify threats. Early alerts are necessary to adequately prevent and respond to cyber attacks. To facilitate information sharing about threats and cyber attacks, INCIBE designed and deployed ICARO, which is based on a malware information sharing platform (MISP) used to share indicators of compromise caused by cyber threats. Using ICARO, Spanish critical operators have a channel that facilitates the anonymization of shared information and access to CERTSI information. This platform also can be federated with other MISPs worldwide.

C. The National Network of Industrial Laboratories (RNLI) is a search platform for information on industrial laboratories with the capacity to experiment and research national industrial infrastructure security solutions. RNLI pursues the dual objectives of promoting innovation in industrial cyber security through collaboration and facilitating the development of solutions that improve the competitiveness of domestic industry.

A tram pulls away from the station in Lodz, Poland. A cyber attack by a teenager caused four trams to derail in 2008.

AFP/GETTY IMAGES

INCIBE is one of the organizers of CyberEx, an annual competition providing different scenarios to test cyber resilience.
INCIBE

EARLY ALERTS ARE NECESSARY TO ADEQUATELY PREVENT AND RESPOND TO CYBER ATTACKS.

RNLI allows operators to find information on national infrastructures and create a point of union between the supply of, and demand for, security in these environments. Other benefits include promoting collaboration and cooperation among all actors involved and facilitating the exchange of expert knowledge within the community.

D. INCIBE collaborates with manufacturers, cyber security companies, laboratories and critical infrastructure operators to develop innovative tools for the improvement of the critical infrastructure's cyber security and CERTSI's detection capabilities.

With these tools, INCIBE and CERTSI can provide new services, such as generating alerts to those operators with vulnerable industrial control devices. Once INCIBE receives an alert from a manufacturer about a specific device, INCIBE identifies those operators that have this type of device and sends them an alert with all of the information required for self-protection.

Other complementary tools allow the detection of industrial control systems that are accessible from the internet, allowing INCIBE to improve its alert services.

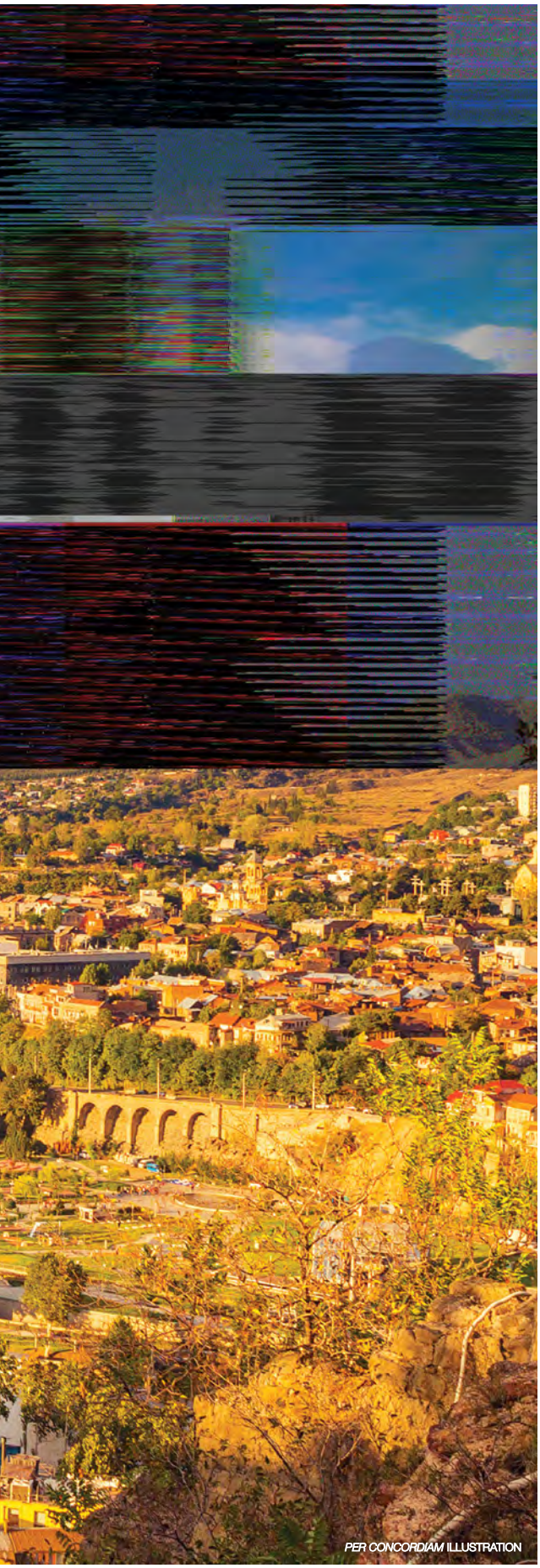
E. As the final element of the strategy, national cyber security exercises in Spain allow for the testing and improvement of the cyber security capabilities of critical infrastructure operators. As part of this initiative, named National CyberEx, several exercises have been carried out. After centering on the banking sector in 2015, the 2016 edition was developed to assess and improve several sectors' resilience to attack, giving participants tangible benefits for their security teams' operations.

Across these exercises, involving all professional roles on the operators' teams, participants improve their response capabilities and strengthen coordination between entities.

Conclusions

The global perspective and nature of the challenges of cyber security in critical infrastructure protection require a comprehensive approach, where a variety of actions are necessary. These actions should cover state-of-the-art technology and manufacturers, current regulations, users and the human factor. Vitally, it also requires perfect coordination among all stakeholders along with a continued commitment to innovation and evolution. □

REBOOTING SECURITY



PER CONCORDIAM ILLUSTRATION

AN INNOVATIVE PLAN FOR PROTECTING GEORGIA'S CRITICAL INFRASTRUCTURE

By Andria Gotsiridze and Maka Petriashvili

In the 21st century, cyberspace has become the fifth domain of conflict, together with air, land, sea and space. Countries increasingly exploit cyberspace to achieve political or military goals or for geopolitical advantage. The number of states successfully developing offensive cyber capabilities is constantly increasing, and cyber warfare is rapidly becoming an integral component of war and conflict.

Russia, especially, has successfully integrated cyber elements into its hybrid war tactics. Its offensive cyber activities encompass all military, diplomatic, political, economic, social, cultural and religious areas, which it uses to exert technical and psychological impacts on its targets. As a result of experiences gained from conducting cyber attacks and information operations in Estonia (2007) and in Georgia (2008), Russia has evolved its offensive cyber tactics to its present-day application in Ukraine. Analysis of these conflicts proves that Russia uses conflict territories as training ranges on which to test its cyber-offensive capabilities.

A banner hangs in the main square in Tbilisi, Georgia, in August 2008, after Russian forces invaded the country. REUTERS

Cyber attacks against Estonia in 2007 were conducted to induce civil unrest. This was the first recognizable attempt to use a cyber attack to influence political processes. By the following year, during the Russo-Georgian war, Russia's cyber strategy had evolved into well-organized attacks, which were synchronized with conventional operations aimed at creating an information vacuum, spreading disinformation and blocking channels of international support for Georgia's government.

Russia's cyber-attack skill set has developed even further during the current conflict in Ukraine. Since the previous operations in Estonia and Georgia, Russia has acquired the use of large cellular operators for secret surveillance, which it uses to determine user location and other data. This data was broadly used for information gathering, psychological impact, and determining and transmitting locations for artillery strikes. For the first time, Russia attacked and shut down Ukrainian energy systems. Over the past two years, Russia has extended its cyber attacks beyond the post-Soviet countries, as hackers associated with various Russian government agencies have targeted election processes in the European Union and the United States.

SERIOUS THREATS

Russian cyber units pose a serious threat to Georgia. They are responsible for offensive cyber operations, including propaganda activities, inserting malware into an adversary's industrial control systems (ICS), and conducting specialized computer network operations and cyber activities on behalf of other units of the Russian armed forces.

Simultaneously, Russia is developing tools for remote access to critical infrastructure ICS. Anonymous actors have already managed to access and disrupt the ICS software of large companies by inserting malware.

After Russia's cyber attacks on Ukraine's energy systems, we can assume that a Russian offensive would not be limited to distributed-denial-of-service (DDoS) attacks, defacement and cyber espionage in future conflicts. There is no guarantee that attackers will not target critical infrastructure, which might lead to massive destruction and human casualties, even though low-level DDoS and defacement themselves may result in disproportionate losses to poorly protected infrastructure.

Together with network disruption and damage, Russia uses destructive cyber-psychological activities to influence an opponent's behavior and perceptions. Militaries prioritize the development of informational capabilities for war, peace or crisis situations to control information content and dissemination mechanisms.

The scale of the cyber threats that Georgia faces is increasing in terms of complexity and diversity, and Russian-orchestrated or -supported cyber attacks can lead to significant material losses and casualties. Cyber propaganda can negatively influence public opinion and perceptions among the Georgian people toward the West and, by forming and strengthening the image of the pro-Russian elite, foment a situation that might lead Russia to risk conventional military operations. Therefore, Georgia should pay special attention to creating and implementing information gathering and analysis mechanisms to better assess the intentions, capabilities and actions of Russia as a destructive cyber power/actor.

Locked Shields 2017, a cyber defense exercise organized by the NATO Cooperative Cyber Defence Centre of Excellence, took place inTallinn, Estonia. It is important for Georgia to participate in international cyber exercises. REUTERS

Ukrainian President Petro Poroshenko speaks in Tbilisi, Georgia, in 2017. Poroshenko, who has moved his country closer to the West, has been targeted several times by hackers. THE ASSOCIATED PRESS

CYBER RESERVE FORCES

It is vital for Georgia to integrate cyber capabilities and network protection into military operations. The country cannot afford not to staff its Armed Forces with qualified cyber specialists. A lack of cyber expertise is a common challenge within the public sector in general, especially for cyber defense. Information technology (IT) intellect is concentrated in the business sector, even in developed countries where public service offers greater pecuniary benefits than in Georgia, with its limited budget. Because cyber security is a common responsibility and critical infrastructure is primarily owned by the private sector, close cooperation between the private and public sectors is imperative, such as an effective public-private partnership model for countering crises during war and peacetime. Moreover, when the principal threat is a nation such as Russia, which broadly uses domestically grown hackers — with false personas such as CyberBercut, the Trolls from Olgino, and internetbots — public-private cooperation is indispensable.

In light of these threats from Russia, establishing a "cyber reserve" — a voluntary mobilization system for IT and cyber specialists employed in the private sector — is a purposeful solution. Such a cyber reserve could enable the state to mobilize nationwide cyber assets during war or crisis situations. Cyber reservists would employ their inherent knowledge and expertise in state emergencies. This system would also benefit the business sector, because IT specialists would have the opportunity to participate in various training and exercises typically available only to employees of state agencies. Such special skill sets are very important to effectively manage crisis situations such as those that resulted from the WannaCry and Petya viruses. As an example of best practices, Lithuania and Austria enlist IT specialists into their reserve forces, and Estonia very successfully deploys the essentially volunteer-based Defence League.

Cyber reservists would be recruited on a volunteer basis. The cyber reserve would consist of IT specialists from banks, internet providers, mobile operators, energy providers or other technology companies. These reservists would voluntarily serve and be called up via the Georgian National Guard. All recruits would be required to be certified in IT education and possess adequate skills and/or expertise to meet pre-established cyber reservist qualifications.

Their training would cover the general principles of information security and specialized cyber security issues. However, reservists would also be trained in basic combat and information operations skills. Cyber reserve service would be an alternative to compulsory military service.

Benefits to the state:

- Cyber defense capabilities enhanced to meet contemporary cyber challenges and threats.
- The Armed Forces acquires additional cyber and information operations capabilities.
- Cyber defense strengthened by integrating highly qualified IT professionals with minimal human resources and financial spending.

Benefits to cyber reservists:

- Opportunities to attend special state-funded training venues and exercises that are closed to the public.
- Opportunities to serve in the reserves as an alternative to compulsory standard military service.
- Maintaining and increasing professional proficiency while serving.
- Serving as a professional during war or crisis situations.

Benefits to the business sector:

- Employee qualifications improved via state-funded training.
- Company infrastructure better protected.
- Company employees exempted from compulsory military service.
- Cyber defense methodology development in business processes.

Projected outcomes:

- Development of additional Armed Forces cyber and information operations capabilities.
- Improvement of cooperation and coordination between public and private sectors.
- Integration of cyber elements into military operations.
- Integration of qualified personnel into national defense with minimal costs.

A cash machine in Ukraine is knocked offline during a wave of cyber attacks against Ukrainian institutions in 2017. Ukraine has been heavily targeted by Russian cyber attacks. EPA

WOUNDED WARRIORS

In addition, the cyber reserve would represent an opportunity to reintegrate wounded warriors into the national defense. Georgia has about 1,500 wounded warriors from the 2008 Russo-Georgian War and from international peacekeeping missions in Afghanistan and Iraq who cannot serve on active duty due to their health. However, with training their inclusion in the cyber reserve would be possible.

Fundamental reasons for including wounded warriors in the cyber reserve:

- Georgia's wounded warriors have a high level of patriotism and desire to serve their country.
- Becoming a cyber defender allows them to reintegrate into society in meaningful ways.
- Their aptitude for tactics and strategy and understanding of physical battle tactics correlate to the cyber battlefield.

What will our wounded warriors gain?

- Remaining in the nation's service.
- Contributing to the enhancement of national cyber defense capabilities.
- Gaining cutting-edge skills in the newest and one of the most important security spheres.
- Continued active lifestyle.
- Compensation for services carried out for the country.

CONCLUSION

Cyberspace is a key element of hybrid tactics, and it is also used more and more widely in today's world, including in Georgia. Therefore, it is important to permanently include the cyber component in military exercises on the national level and to ensure that Georgia's state agencies and the private sector participate together in international cyber exercises. Effective cyber defense requires close cooperation between national agencies and private companies.

A cyber reserve project can and should be launched to provide strong support to this cooperation and to develop national cyber capabilities. Integration of private sector IT professionals into critical infrastructure protection will provide Georgia an adequate response capability to the destructive cyber actions of a powerful aggressor. □

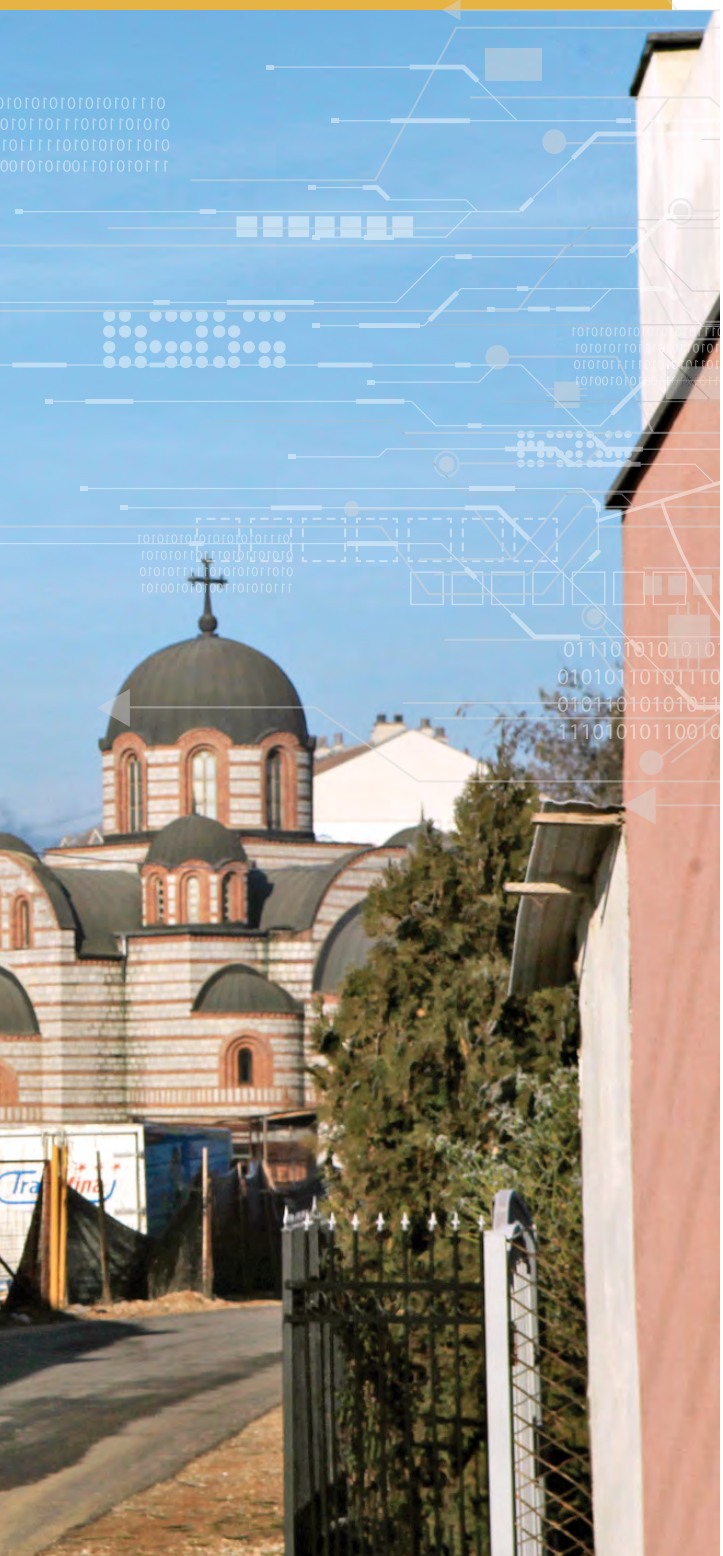
AFP/GETTY IMAGES

A PRESENT CONCERN

AS INTERNET USAGE SOARS, KOSOVO MUST HARDEN ITS DEFENSES

By Hafize Bajrami
IT chief, Ministry for the Kosovo Security Force

Today, the internet is part of work and life for many millions of people worldwide. With the rapid developments in technology, cyber security is a serious concern. Most services in the public and private sectors are conducted via the internet, where users are exposed to threats posed by viruses, malware, cyber espionage and phishing.



Smoke billows from the coal-powered power plant in Obilić near Pristina, Kosovo. Attacks on power plants endanger the public. REUTERS

Kosovo has experienced a rapid growth in the number of internet users and now has a market penetration similar to that of many European Union countries. Cyber crime has been identified as one of the global threats that may affect the security of Kosovo, a concern revealed in the government's 2014 report, "Analysis of the Strategic Security Sector Review of the Republic of Kosovo." Based on this, Kosovo has begun to develop greater cyber security defense capabilities. As is the case with many other countries, the most important areas in need of protection are critical infrastructure (CI) and critical information infrastructure (CII).

The protections include legal frameworks, strategies and policies, and identifying stakeholders and mechanisms responsible for various aspects of CI and CII. Because of the ubiquitous exposure to cyber threats, it is imperative that Kosovo reviews technology investment priorities, with particular attention to security and harmonization of legal frameworks for dealing with network security incidents and data protection. Legal frameworks must be harmonized along national and international vectors because cyber crime is not restricted to conventional markers such as borders, nationality, gender and age.

CII must be identified exhaustively by all governmental institutions. No comprehensive list of CII exists in Kosovo. A law on CI protection was drafted in 2016. This draft law transposes fully the EU Council Directive 2008/114/EC on the identification and designation of European CI and the assessment of steps needed to improve its protection.

According to this law, the identification and prioritization of national CI shall be led by the Ministry of Internal Affairs in consultation and cooperation with security institutions, government and nongovernmental institutions, public and private owners and operators, and key international stakeholders. It is of utmost importance to identify and assess the real CII within the country and to take all necessary measures to protect it.

LEGAL FRAMEWORK

The National Cyber Security Strategy and Action Plan for implementing that strategy was approved by the Assembly of Kosovo in early 2016. Kosovo also has laws that cover many cyber security-related issues, including preventing and fighting cyber crime, information society services and government bodies, electronic communications and protection of personal data.

The primary legal framework for dealing with cyber crime or cyber incidents is found in the criminal code of Kosovo and the criminal procedure code. There is also an Emergency Management Agency law governing national coordination and interoperability, from which emergency response plans are derived. Security institutions respond to crises based on emergency response plans, which are more focused in responding to natural disasters and other emergencies than cyber incidents. For cyber security incidents, Kosovo must update this plan or draft a more effective one. Each institution has its respective administrative instructions

and standard operating procedures or guidelines in place for the use and protection of data networks.

STAKEHOLDERS AND MECHANISMS

As part of the national strategy, the National Cyber Security Council was established in 2016 as the highest governing body for cyber security. The council is led by the deputy minister of the Ministry of Internal Affairs and consists of representatives from the following institutions: the Ministry of Internal Affairs; the Kosovo Police; the Kosovo Forensics Agency; the Ministry for Kosovo Security Forces; the Kosovo Intelligence Agency; the Agency for Information Society; the Kosovo Security Council; the Ministry of Justice; the Kosovo Prosecutorial Council; the Kosovo Judicial Council; the Ministry of Finance; Kosovo Customs; the Ministry of Education, Science and Technology; the Ministry of Foreign Affairs; the Regulatory Authority of Electronic and Postal Communications (RAEPC); and the Central Bank of Kosovo.

The National Computer Emergency Readiness Team (CERT) was established under RAEPC and is trying to achieve needed capacities in terms of human and technical resources, infrastructure and services. Other government institutions are also establishing CERTs for their needs.

EDUCATION, TRAINING AND EXERCISES

Dealing with rapid technological developments and new information technology services is a challenge to Kosovo's public and private sectors. The Ministry of Education has underscored communication and technology as a priority. An example of this prioritization is seen in the emphasis on information and communications technology (ICT) and security issues in the curricula for all levels of education. This emphasis is reflected in efforts to build cyber security programs for primary and secondary schools.

For government users of ICT, the Kosovo Institute for Public Administration has implemented training policies developed by the Ministry of Public Administration. That ministry is conducting annual training for standard users in data security fields based on the varying requests of individual ministries and other government institutions.

An important part of national coordination and interoperability is to design scenarios and conduct joint exercises through which the institutions involved can test their capacity to respond to contemporary challenges. These exercises improve incident response capacity for various threats, whether at the national or institutional level. After the national security strategy was approved, each institution conducted cyber exercises to raise user awareness and exercises were planned to test interagency readiness cooperation.

RECOMMENDATIONS

Improving cyber security can be achieved by understanding:

- The national cyber security strategy was drafted based on European Union Agency for Network and Information Security (ENISA) guidelines. Other laws have yet to be adopted to better synchronize strategy, technology development and international legal frameworks between Kosovo and international entities such as the EU, NATO, the United Nations and other international organizations.
- All institutions responsible for cyber security must develop and harmonize policies and procedures to protect critical data and infrastructure. Those policies should bear sufficient authority to ensure interoperability among institutions inside and outside of Kosovo.
- Greater investment in the National CERT is necessary to make it fully operational with adequate personnel, equipment and tools, and training, which in turn would make it eligible for accreditation in Trusted Introducer (established by the European CERT community to address common needs and support all security and incident response teams) and the global Forum of Incident Response and Security Teams, or FIRST.
- The National CERT should be empowered to establish cooperation with regional and international CERTs.
- A rigorous assessment to identify CII and take all necessary measures to protect it is needed.
- Public sector cooperation and information-sharing venues with key private sector partners, through effective public-private partnership models, should be encouraged.
- Organizing and participating in international cyber security activities, such as conferences, seminars and workshops, is beneficial. So are scenarios and cyber security exercises for all relevant institutions with an aim to test interoperability within the country.
- It is important to develop training curricula within civil educational institutions to teach effective data protection and privacy measures to online users with special emphasis on protecting children online, and to develop programs to raise parental awareness of online risks.
- There is a need to organize awareness campaigns and update current ICT curricula at pre-university levels with cyber security modules. ENISA's Network and Information Security Directive and the U.S. National Institute of Standards and Technology's National Initiative for Cybersecurity

A construction worker prepares to open a newly constructed highway in Kosovo that is a centerpiece of the national transport system.

THE ASSOCIATED PRESS

Education serve as ready examples for raising cyber security awareness.

- It is essential to train and certify personnel involved with information security in all government institutions and private companies dealing with ICT.

CONCLUSION

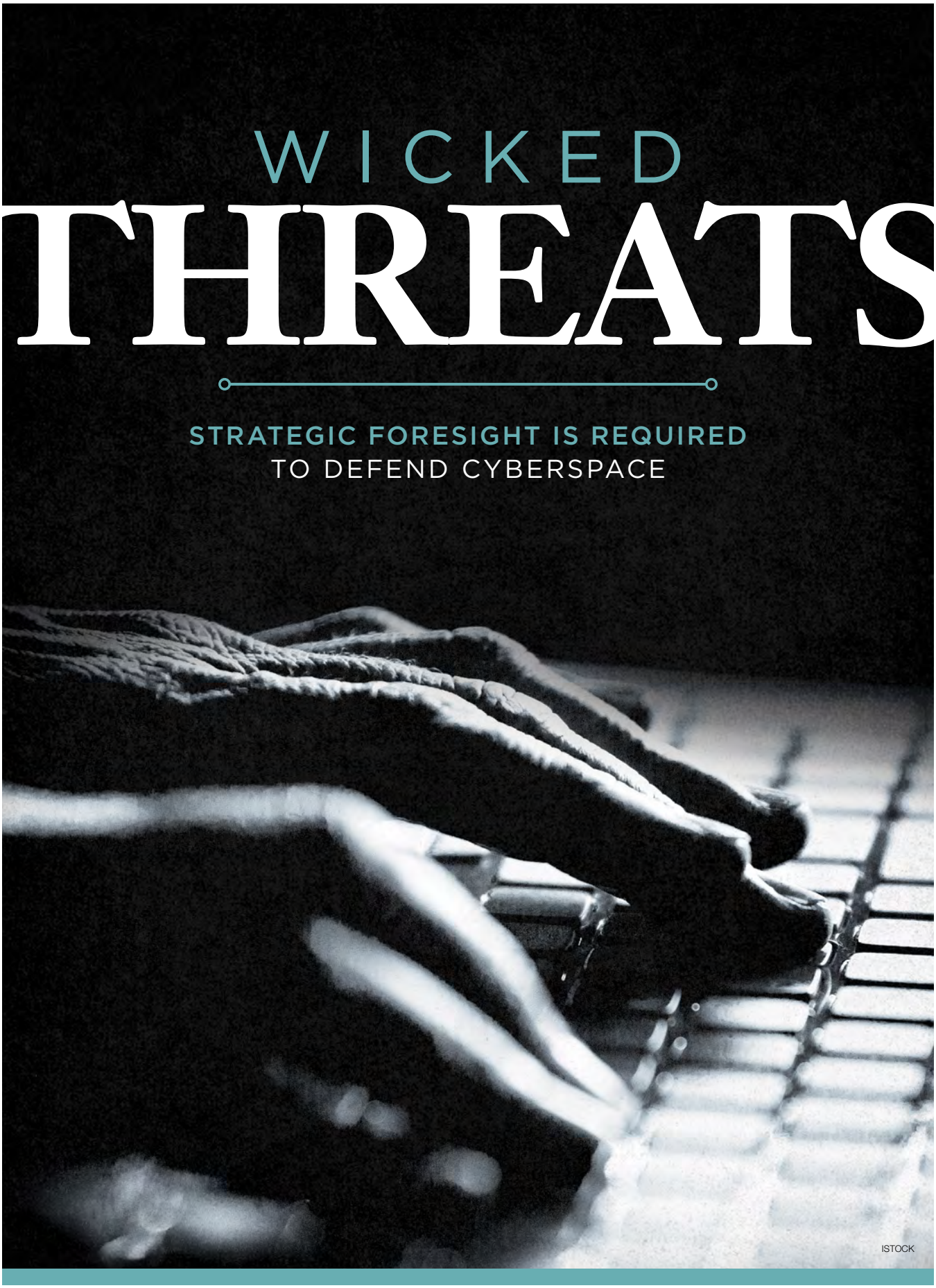
Cyber crime continues to pose the most significant challenges for Kosovo's institutions. The country has taken concrete steps to establish the legal infrastructure to prevent and combat all forms of cyber crime, but many challenges remain, especially in technical response capabilities, which is a relatively new phenomenon in Kosovo.

There is an ongoing need to reinforce the foundations of institutions involved in protecting against and prosecuting cyber crime by modernizing their technological equipment, supporting international cooperation in information sharing, and properly empowering the agencies best-placed to address cyber threats. Another need is to improve coordination between law enforcement authorities and technical personnel to better address the complexities of cyber crimes.

Finally, a robust cyber security awareness training, education and exercise capability will need to further mature to fully identify and mitigate Kosovo's CI and CII security shortfalls. Incorporation of cyber awareness curricula into formative education venues from an early age will foster a cyber security capacity-building environment where baseline risk awareness will meaningfully add to Kosovo's cyber security architecture and opportunities. □

WICKED THREATS

STRATEGIC FORESIGHT IS REQUIRED TO DEFEND CYBERSPACE



ISTOCK

By **Maj. Walbery Nogueira de Lima e Silva**, Brazilian Army

Historically, the adoption of new technologies has resulted in three important revolutions in industry. The first revolution came with the advent of steam-powered machines; the second with the harnessing of electricity; and the third with the advent of computers, leading to automation of production processes.

Industry 4.0 is the current trend, using technology related to cyber-physical systems, the internet of things and cloud data storage. Through these innovations, it is now possible to build "smart factories," integrating human decision-making with computerized automation, making the manufacturing process more efficient and effective.

Some characteristics of Industry 4.0 are interoperability between machines and people; information transparency; technical assistance that allows systems to support human decision-making or to do hazardous tasks; and decentralized, autonomous decision-making for specific activities using cyber tools.

EVOLUTION OF WAR

One of the principles of war and of joint operations is surprise. Historically, the use of an "offset" strategy to create advantages has often been key to quickly prevailing over an enemy. The first offset (nuclear weapons) and second offset (stealth and precision-guided munitions) were used by the United States and NATO to counter Soviet/Warsaw Pact strategic advantages during the Cold War.

The third offset relies on next-generation technologies and concepts to assure strategic superiority over adversaries by using, for instance, advances in artificial intelligence and autonomy integrated into battle networks, according to the U.S. Department of Defense. Modern war is complex and demands effective command and control of military forces with fast and decentralized decision-making processes. It is necessary to be aware of everything that is happening on the battlefield with C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance). Third-offset technologies enable this.

Cyberspace is one of five interdependent domains, along with the physical domains of air, land, maritime and space, but it overlaps the other four in modern war. Joint forces in a contested and disordered world demand increasing cyber capability that will bring the most important combat into the "virtual theater," aiming to defeat the adversary's network and computational systems.

WORLDWIDE THREATS

In the globalized world of the information age, there is a trend of borderless integration in cyberspace. Every year, information and communications technology (ICT) touches more segments of society on public, private and individual levels. Governments, citizens and multinational corporations link their systems worldwide through ICT in an interdependent net that relies on several physical and virtual hubs that have vulnerabilities and can be exploited for cyber terrorism, crime, espionage and hacktivism purposes, according to the European Union Agency for Network and Information Security.

Cyberspace underpins modern society and provides critical support to the global economy, but is permeated with tremendous potential vulnerabilities that not only can undermine personal privacy, but can damage the operations of critical infrastructure, affecting cities, states and even an entire country.

Currently, there are about 3.6 billion internet-connected people on the planet and an increasing number of internet-of-things users. This is one of the points most vulnerable to cyber attacks, because many ordinary users do not know how to correctly set and use security measures for their connected devices, opening doors to cyber criminals. Due to the large number of vulnerabilities, cyber exploitation can have

The 5th Brazilian Computer Security Incident Response Team Forum, held in September 2017 in São Paulo, brought together experts from the private sector, academia and government to share information and lessons learned during the Rio 2016 Olympic Games. BRAZILIAN ARMY

low cost of entry, ubiquity and relative anonymity, Phil Williams explains in the book, *Cyberspace: Malevolent Actors, Criminal Opportunities and Strategic Competition*. Perpetrators can act alone against a single target or in a wicked chain, targeting complex systems and using, for instance, advanced persistent threats.

According to the Brazilian Cyber Defense Military Doctrine, critical infrastructure (CI) consists of facilities, services, goods and systems that, if harmed, disrupted or destroyed, could seriously impact the government, social and economic sectors and have international impacts as well. Depending on the level of severity, the vulnerability exploited and the damage to any of these sectors, the country's national security and economy could be negatively affected. Therefore, cooperation among all cyber defense partners is important.

There have been several recent examples of this theme. In 2007, a sequence of cyber attacks swamped numerous Estonian websites, including banks, government ministries, newspapers and broadcasters, causing serious damage to the country.

A lack of cyber security and cyber policy enhances the threats (who is attacking), vulnerabilities (the weaknesses they are attacking) and the impact (what the attack does). For these reasons, there should be unified international efforts employing a comprehensive approach to enhance cyber protection measures within the scope of adequate global laws.

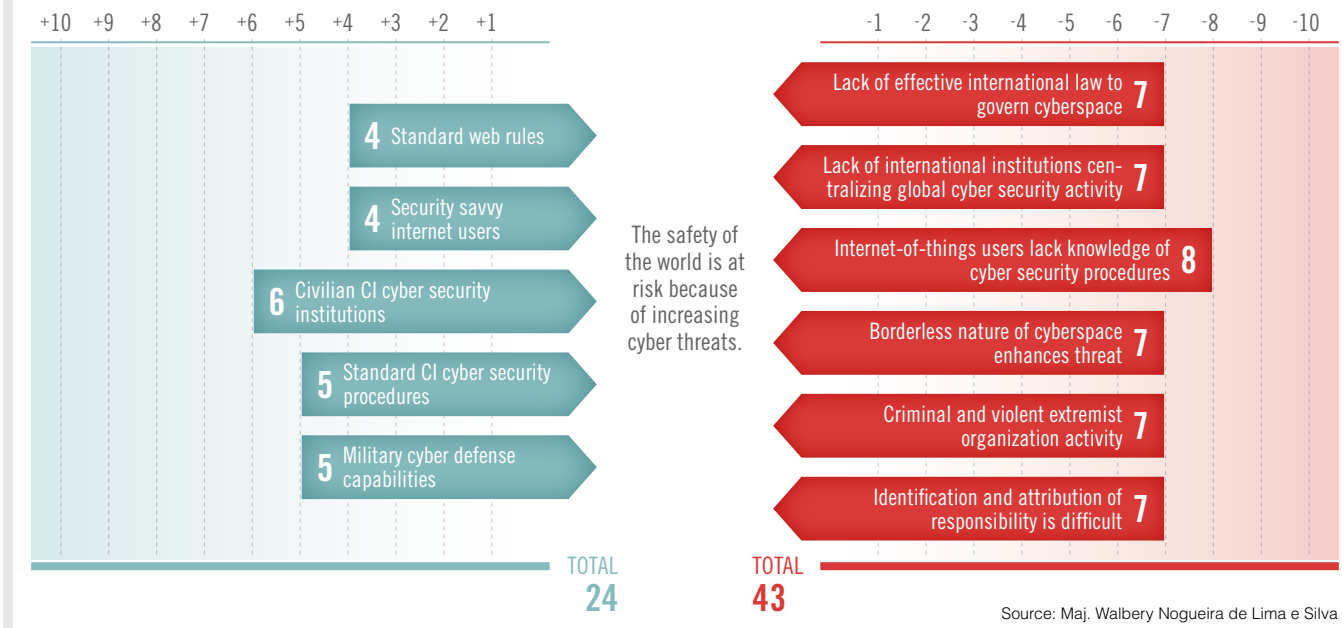
A man uses a 3-D printer during a February 2017 convention of internet users in São Paulo, Brazil. New technologies and the rapidly expanding internet of things require more proactive cyber security measures. REUTERS

STRATEGIC FORESIGHT

To fairly address the enormous challenge of protecting cyberspace demands an accurate understanding of the operational environment. Among the various tools available, the strategic foresight approach is a good way to see the big picture through models such as force field analysis, future wheels and implication trees.

A. Force field analysis: This graphically depicts intensity and relationships that involve powers, actors, interests, etc., related to a specific problem. For example, Figure 1 concludes that cyber threats endanger the world community.

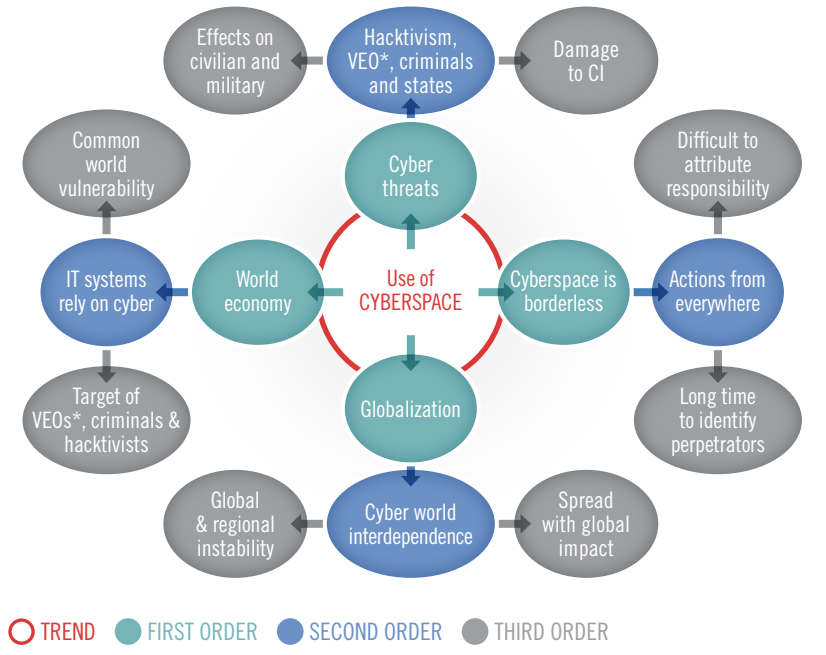
Threats in cyberspace worldwide Force Field Analysis *Fig.* 1



Source: Maj. Walbery Nogueira de Lima e Silva

Futures wheels

Fig. 2

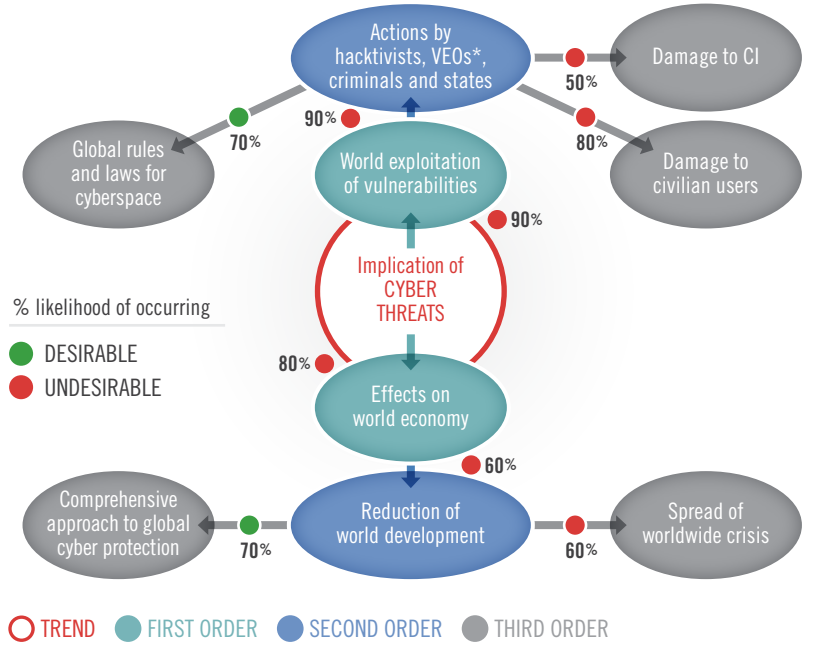


* Violent extremist organizations

Source: Maj. Walbery Nogueira de Lima e Silva

Implication Tree

Fig. 3



* Violent extremist organizations

Source: Maj. Walbery Nogueira de Lima e Silva

B. Futures wheels: This diagram highlights trends and depicts the potential consequences when cyberspace is affected by various factors, as shown in Figure 2.

C. Implication tree: This helps identify the desirable and undesirable conditions as well as the likelihood of those conditions occurring, as shown in Figure 3.

CONCLUSION

Cyberspace does not have borders or limits, and criminals, hacktivists, violent extremist organizations or malevolent actors can increase instability around the world, affecting civilians and militaries wherever they are. The cyber domain underpins modern society, providing critical support to the global economy, civil infrastructure, public safety and national security.

The problem is troublesome. Addressing it calls for a long-term, steady perspective, requiring unity and cooperation among countries, international organizations, nongovernmental organizations and private-sector actors, incorporating a comprehensive, whole-of-government approach.

To avoid the undesirable conditions highlighted by the implication tree, the following actions are necessary:

- Share information through an integrated system to expeditiously mitigate and solve cyber threats.
- Promote collective approaches and share best practices.
- Increase awareness of the magnitude of cyber security challenges.
- Review and critique cyber security themes with a focus on strategy, policy, legal frameworks and international cooperation.
- Instill a whole-of-government approach to cyber security.
- Increase public-private cooperation.
- Involve the academic community worldwide in expanding information security research.
- Provide proactive coordination support from the international community.

International cyber cooperation is important to upholding freedom of expression and association, respect for property, intellectual property rights and privacy, and to preventing arbitrary or unlawful interference with those rights.

Finally, trust is the key value that allows building long-term and effective cooperation among a variety of stakeholders in the cyber domain. □

HACKING THE PENTAGON

A REGIONAL CONFERENCE AND FRIENDLY PENTAGON CYBER SLEUTHS HELP BOLSTER SECURITY

BY *PER CONCORDIAM* STAFF

PHOTOS BY COL. LEERNEST M. RUFFIN/U.S. AIR FORCE

Safeguarding against cyber attacks is critical to the defense of any nation. Innovation is key as enemy tactics evolve and technological advances reveal new vulnerabilities. That's why the U.S. Department of Defense (DOD) launched the "Hack the Pentagon" program, a bold initiative to shore up cyber defenses.

Launched in 2016, the program was the first of its kind for the federal government. It empowers individuals to hunt for bugs and vulnerabilities in DOD websites available to the public.

"We know that state-sponsored actors and black-hat hackers want to challenge and exploit our networks," former U.S. Secretary of Defense Ash Carter said at the program's launch. "What we didn't fully appreciate before this pilot was how many white-hat hackers there are who want to make a difference, who want to help keep our people and our nation safer."

Managed by the DOD's digital service team, about 14,000 "hackers" registered to participate in the pilot program. They agreed to follow certain rules and in return were paid when finding legitimate vulnerabilities on DOD platforms. Websites such as Defense.gov, DoDlive.mil, DVIDSHUB.net (Defense Video Imagery Distribution System) and MyAFN.net (My American Forces Network Online) were among those chosen as targets.

"When it comes to information and technology, the defense establishment usually relies on closed systems," Carter said. "But the more friendly eyes we have on some of our systems and websites, the more gaps we can find, the more vulnerabilities we can fix, and the greater security we can provide to our warfighters."

The first vulnerability report was filed just 13 minutes after the pilot launched, and within six hours there were 200 reports. A total of $75,000 was paid for reports submitted over a month.

One of the hackers — a high school student — said he was thankful for the unique opportunity. "It was a great experience," David Dworken said. "I just started doing more and more of these bug bounty programs and found it rewarding — both the monetary part of it and doing something that is good and beneficial to protect data online in general."

The program was considered a huge success. Hundreds of vulnerabilities were discovered that had been missed by government teams, including more than a dozen considered high risk, said Kate Charlot, principal director for cyber policy within the U.S. Office of the Secretary of Defense. She shared the program with cyber security leaders and experts from the Middle East during the U.S. Central Command's (CENTCOM's) Central Region Communications Conference (CRCC) in April 2017 in Alexandria, Virginia, in the United States. The U.S. Army is planning a similar program.

The DOD has also created a procedure for people to report vulnerabilities on any DOD public site. Like the bug bounty program, it's the first of its kind for the U.S. federal government, basically the equivalent of a digital "see something, say something," campaign.

Increasing Vulnerabilities

The need for these programs is growing exponentially. Children's toys, refrigerators, home security alarms and traffic lights are just a few of the abundant internet-enabled devices present in our daily lives. While each new item offers convenience and innovation to people across the world, there is a trade-off: Web-based systems and products are vulnerable to hacking.

"There is an absence of international laws regarding cyber security today. With military, the laws are very clear regarding a country's sovereignty. With cyber, it's still open."

— Mohammad Altura

Mohammad Altura, executive board member of Kuwait's Communications and Information Technology Regulatory Authority, gives a presentation on his country's progress in cyber security during a 2017 conference.

"You must understand your critical assets and their associated vulnerabilities. You must talk about the risk to the mission and the risk to critical assets. This is important for commanders."

— U.S. Army Maj. Gen. Mitchell Kilgo

U.S. Army Maj. Gen. Mitchell Kilgo, director of Command, Control, Communications and Computer Systems at U.S. Central Command, speaks with his counterpart from Saudi Arabia, Maj. Gen. Riyadh bin Abdul Aziz Al-Dugheither, on the sidelines of a 2017 cyber conference.

TOP 10 IN CYBER SECURITY

The Global Cyber Security Index (GCI) 2017 shows that commitment to cyber security is not tied to a geographic location. Three of the countries ranked in the Top 10 are from the Indo-Pacific, two are from Europe and two are from North America. The other three are from Africa, the Arabian Peninsula and the Commonwealth of Independent States.

COUNTRIES ARE RANKED BASED UPON THEIR PROGRESS IN FIVE KEY AREAS.

1. **Legal:** The existence of legal institutions and frameworks for cyber security.
2. **Technical:** The existence of technical institutions and frameworks dealing with cyber security.
3. **Organizational:** The existence of policy coordination institutions and strategies for cyber security at the national level.
4. **Capacity Building:** The existence of research and development, education and training programs; certified professionals and public sector agencies fostering capacity building.
5. **Cooperation:** The existence of partnerships, cooperative frameworks and information sharing networks.

Air-conditioning systems that cool the rooms storing government computer servers can be interrupted, causing network disturbances. A doll that records voices to entertain and comfort children can record private conversations inside homes. As technology advances, the number of potential vulnerabilities also grows, increasing the importance of preparing for cyber breaches.

Creating opportunities for military, academic, government and industry experts to collaborate and gain new perspectives on each other's roles in national security is imperative to address these challenges. The CRCC was one of these opportunities; it focused on cyber incident response. The relationships developed during the conference enable organizations to recover more quickly and with less damage when an incident occurs.

"I believe our best defense is to be proactive," CENTCOM Deputy Commander Lt. Gen. Charles Brown Jr. said during the conference. He explained that each country is stronger by collaborating with various organizations within the country and with cyber experts across the world.

To do this requires dismantling a culture of "information silos" that exists in many organizations. This will help leaders make decisions based on all available information, explained U.S. Army Maj. Gen. Mitchell Kilgo, director of CENTCOM's Command, Control, Communications and Computer Systems. "You must understand your critical assets and their associated vulnerabilities," Kilgo said. "You must talk about the risk to the mission and the risk to critical assets. This is important for commanders."

Representatives from private companies and academia gave presentations at the conference. Senior government representatives spoke about the best practices in their countries, providing insights into topics worthy of future discussions.

"In Iraq, the growth of the internet's popularity — for security, business and personal use — coincided with a lack of secure cyber infrastructure," explained Maj. Gen. Mahdi Yasir Zubaidi, director of military communication for Iraq's Ministry of Defense. "This raised awareness of the need to understand the dangers of cyber crimes accompanying every new technological development, especially in the context of society's transformation into a cyber community.

Experts said a good cyber defense takes more than just software. To better protect networks and identify vulnerabilities, system administrators must be trained to understand how adversaries think and how to "hunt" them down in a network.

Countries such as Kuwait have had success in developing a whole-of-government approach to cyber security. Mohammad Altura, executive board member of Kuwait's Communication and Information Technology Regulatory Authority, gave a detailed presentation about his country's strategy development process. Kuwait has identified objectives to focus on over the next three years. The three principle strategic initiatives are to promote a culture of cyber security in Kuwait; to safeguard and continually maintain the security of national assets including critical infrastructure, information, communication technologies and the internet; and to promote the cooperation, coordination and information exchange with local and international bodies in the field of cyber security.

"There is an absence of international laws regarding cyber security today," Altura said. "With military, the laws are very clear regarding a country's sovereignty. With cyber, it's still open." □

Information from the U.S. Department of Defense and the cyber security firm HackerOne was used in this report.

	Country	GCI Score	Legal	Technical	Organizational	Capacity Building	Cooperation
1	Singapore	0.92	0.95	0.96	0.88	0.97	0.87
2	United States	0.91	1	0.96	0.92	1	0.73
3	Malaysia	0.89	0.87	0.96	0.77	1	0.87
4	Oman	0.87	0.98	0.82	0.85	0.95	0.75
5	Estonia	0.84	0.99	0.82	0.85	0.94	0.64
6	Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
7	Australia	0.82	0.94	0.96	0.86	0.94	0.44
8	Georgia	0.81	0.91	0.77	0.82	0.90	0.70
9	France	0.81	0.94	0.96	0.60	1	0.61
10	Canada	0.81	0.94	0.93	0.71	0.82	0.70

Key: 1 is the maximum score

Source: International Telecommunication Union

STRENGTH IN NUMBERS

PERSPECTIVES ON THE AFRICA ENDEAVOR 2017 SYMPOSIUM

ISTOCK

By *Capt. Domingos Tavares,* Armed Forces of Cape Verde PHOTOS BY REUTERS

Internet and mobile technologies permeate Africa, transforming all aspects of human life on the continent and inducing a transference of humanity to cyberspace. The challenges of digitalization are apparent as cyber crime meets a deficit of cyber security laws, and combatting traditional crimes requires transnational interoperability. Africa Endeavor 2017, held in Malawi, underscored some significant cyber security shortfalls that most of the continent has yet to consider. Senior representatives of many African nations attend the annual symposium co-hosted by U.S. Africa Command and an African partner country.

The presentations generated strong audience engagement and a tremendous interest in comprehending not only the parameters of cyber security, but how to begin addressing the problems. It is this author's view that countries such as Cape Verde that have already begun to address cyber security issues must be available to help others by becoming partners in the fight against cyber crime. But the most important step is to convince policymakers of the importance of cyber security and the need to create laws that, if compatible with international partners, can effectively address cyber crime.

During Africa Endeavor, representatives from the Netherlands effectively illustrated that cyber security often begins with the user, whose ignorance or carelessness can expose all manner of personal data on digital platforms. The presentation emphasized the importance of being alert when using certain websites and the importance of having a strong and secure password.

The conference also addressed the nature of transnational organized crime, which now has a cyber security component. Nations must contemplate the many consequences associated with maritime piracy, illegal fishing, and the trafficking of people, animals and goods. The communication and cooperation encouraged at Africa Endeavor, where the objective is to analyze and overcome interoperability challenges, can play a fundamental role in solving these challenges.

In 2016, Cape Verde approved the National Strategy for Cybersecurity, making clear that it is key to the country's development. The strategy's primary objective is to protect the country from cyber threats and crimes by assigning responsibilities to national, international and global actors.

Cyber security is key to development because the country is heavily dependent on communication technologies, and its vulnerabilities are increasing as a result of this dependency. We have an electronic governance structure, a high

Clients browse the internet at a cyber cafe in Mogadishu, Somalia, in 2017. With the African population becoming ever more connected, the need for cyber security is essential.

Taiwanese and Chinese nationals arrested on suspicion of telecommunications fraud listen to a translator in Nairobi, Kenya. Cyber fraud is a growing concern as Africa expands its digital footprint.

saturation of internet subscribers (about 70 percent of the population), and a society that intertwines personal and business communications.

The strategy addresses the issue of cyber security for citizens and for public and private institutions. It sends a strong message that we will not allow Cape Verde to become a paradise for cyber criminals drawn to countries where there are no legal consequences for cyber crime.

The country has been working toward international cooperation with the African Union and the Economic Community of West African States, with the support of partners such as the United States. A major objective is to create a national cyber security center that will include a computer emergency response team that should serve in all sectors, including national defense.

Cyberspace is an open world in which the crime and the criminal are not necessarily located in the same place. The targets may be civilian, military or paramilitary infrastructures, and a decreasing distinction between these factors is becoming more evident. Therefore, it is essential that the military is capable of dealing with cyber threats that jeopardize security, and it is also essential that there be information sharing with the civilized world because cooperation in the digital domain is essential.

Africa Endeavor 2017 provided a forum for addressing national and regional security concerns on the African continent, and it remains a solid foundation upon which to build further integration and interoperability capabilities to address internet-based threats, cyber security shortfalls and the continually changing nature of today's criminal activities. □

A DOUBLE DOSE
ONLINE

Read current and past issues of *per Concordiam*

http://perconcordiam.com

Submit articles, feedback and subscription requests to the Marshall Center at: editor@perconcordiam.org

Get the freshest *global security news* updated weekly:

transnational weekly

http://www.marshallcenter.org

GEORGE C. MARSHALL EUROPEAN CENTER FOR SECURITY STUDIES
DEMOCRATIA PER FIDEM ET CONCORDIAM

Resident Courses

Democratia per fidem et concordiam
Democracy through trust and friendship

Registrar
George C. Marshall European Center
for Security Studies
Gernackerstrasse 2
82467 Garmisch-Partenkirchen
Germany
Telephone: +49-8821-750-2327/2229/2568
Fax: +49-8821-750-2650

www.marshallcenter.org
registrar@marshallcenter.org

Admission
The George C. Marshall European Center for Security Studies cannot accept direct nominations. Nominations for all programs must reach the center through the appropriate ministry and the U.S. or German embassy in the nominee's country. However, the registrar can help applicants start the process. For help, email requests to: registrar@marshallcenter.org

PROGRAM ON APPLIED SECURITY STUDIES (PASS)

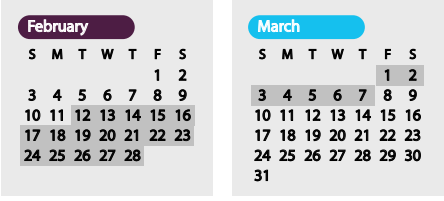
The Marshall Center's flagship resident program provides graduate-level education in security policy, defense affairs, international relations and related topics such as international law and counterterrorism. A theme addressed throughout the program is the need for international, interagency and interdisciplinary cooperation.

PASS 19-19
Sept. 10 -
Nov. 20, 2019

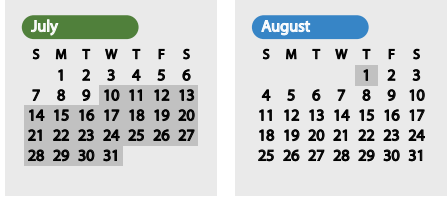
PROGRAM ON COUNTERING TRANSNATIONAL ORGANIZED CRIME (CTOC)

This resident program focuses on the national security threats posed by illicit trafficking and other criminal activities. The course is designed for government and state officials and practitioners who are engaged in policy development, law enforcement, intelligence and interdiction activities.

CTOC 19-6
Feb. 12 -
Mar. 7, 2019



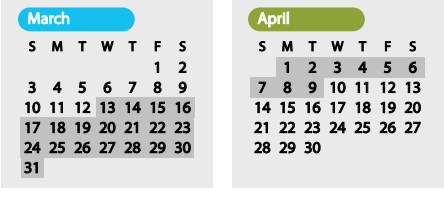
CTOC 19-16
July 10 -
Aug. 1, 2019



PROGRAM ON TERRORISM AND SECURITY STUDIES (PTSS)

This program is designed for government officials and military officers employed in midlevel and upper-level management of counterterrorism organizations and will provide instruction on both the nature and magnitude of today's terrorism threat. The program improves participants' ability to counter terrorism's regional implications by providing a common framework of knowledge and understanding that will enable national security officials to cooperate at an international level.

PTSS 19-7
Mar. 13 -
Apr. 9, 2019



PTSS 19-18
Aug. 7 -
Sept. 4, 2019

PROGRAM ON CYBER SECURITY STUDIES (PCSS)

The PCSS focuses on ways to address challenges in the cyber environment while adhering to fundamental values of democratic society. This nontechnical program helps participants appreciate the nature of today's threats.

PCSS 19-2
Dec. 4 - 20, 2018

December

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

SEMINAR ON REGIONAL SECURITY (SRS)

The seminar aims at systematically analyzing the character of the selected crises, the impact of regional actors, as well as the effects of international assistance measures.

SRS 19-8
Apr. 24 -
May 17, 2019

April

S	M	T	W	T	F	S
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

May

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

SENIOR EXECUTIVE SEMINAR (SES)

This intensive seminar focuses on new topics of key global interest that will generate new perspectives, ideas and cooperative discussions and possible solutions. Participants include general officers, senior diplomats, ambassadors, ministers, deputy ministers and parliamentarians. The SES includes formal presentations by senior officials and recognized experts followed by in-depth discussions in seminar groups.

SES 19-15
June 24 - 28, 2019

June

S	M	T	W	T	F	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30						

Alumni Programs

Dean Reed
Director, Alumni Programs
Tel +49-(0)8821-750-2112
reeddg@marshallcenter.org

Alumni Relations Specialists:

Drew Beck
Southeast Europe
Languages: English, French
Tel +49-(0)8821-750-2291
ryan.beck@marshallcenter.org

Christian Eder
Western Europe
Languages: German, English
Tel +49-(0)8821-750-2814
christian.eder@marshallcenter.org

Marc Johnson
Central Asia, South Caucasus, Russia, Moldova, Ukraine, Belarus - Cyber Alumni Specialist
Languages: English, Russian, French
Tel +49-(0)8821-750-2014
marc.johnson@marshallcenter.org

Christopher Burelli
Central Europe, Baltic States - Counterterrorism Alumni Specialist
Languages: English, Slovak, Italian, German
Tel +49-(0)8821-750-2706
christopher.burelli@marshallcenter.org

Donna Janca
Africa, Middle East, Southern and Southeast Asia, North and South America - CTOC Alumni Specialist
Languages: English, German
Tel +49-(0)8821-750-2689
nadonya.janca@marshallcenter.org

mcalumni@marshallcenter.org

Contribute

Interested in submitting materials for publication in *per Concordiam* magazine? Submission guidelines are at **http://tinyurl.com/per-concordiam-submissions**

Subscribe

For more details, or a **FREE** subscription to *per Concordiam* magazine, please contact us at **editor@perconcordiam.org**

Find us

Find *per Concordiam* online at:
Marshall Center: **www.marshallcenter.org**
Twitter: **www.twitter.com/per_concordiam**
Facebook: **www.facebook.com/perconcordiam**
GlobalNET Portal: **https://members.marshallcenter.org**
Digital version: **http://perconcordiam.com**

The George C. Marshall European Center for Security Studies in Garmisch-Partenkirchen, Germany

MARSHALL CENTER