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.

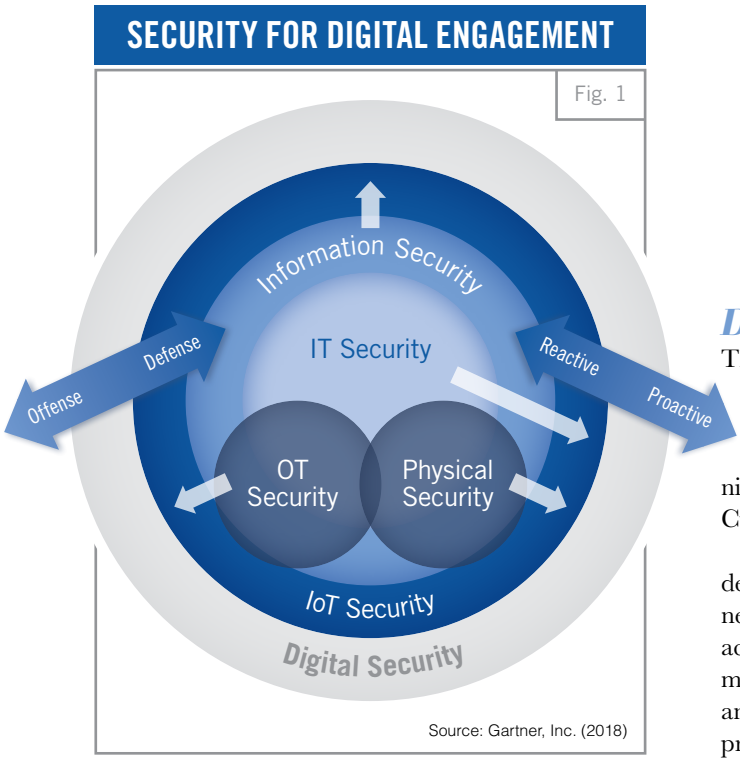
Defining cyber security

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.

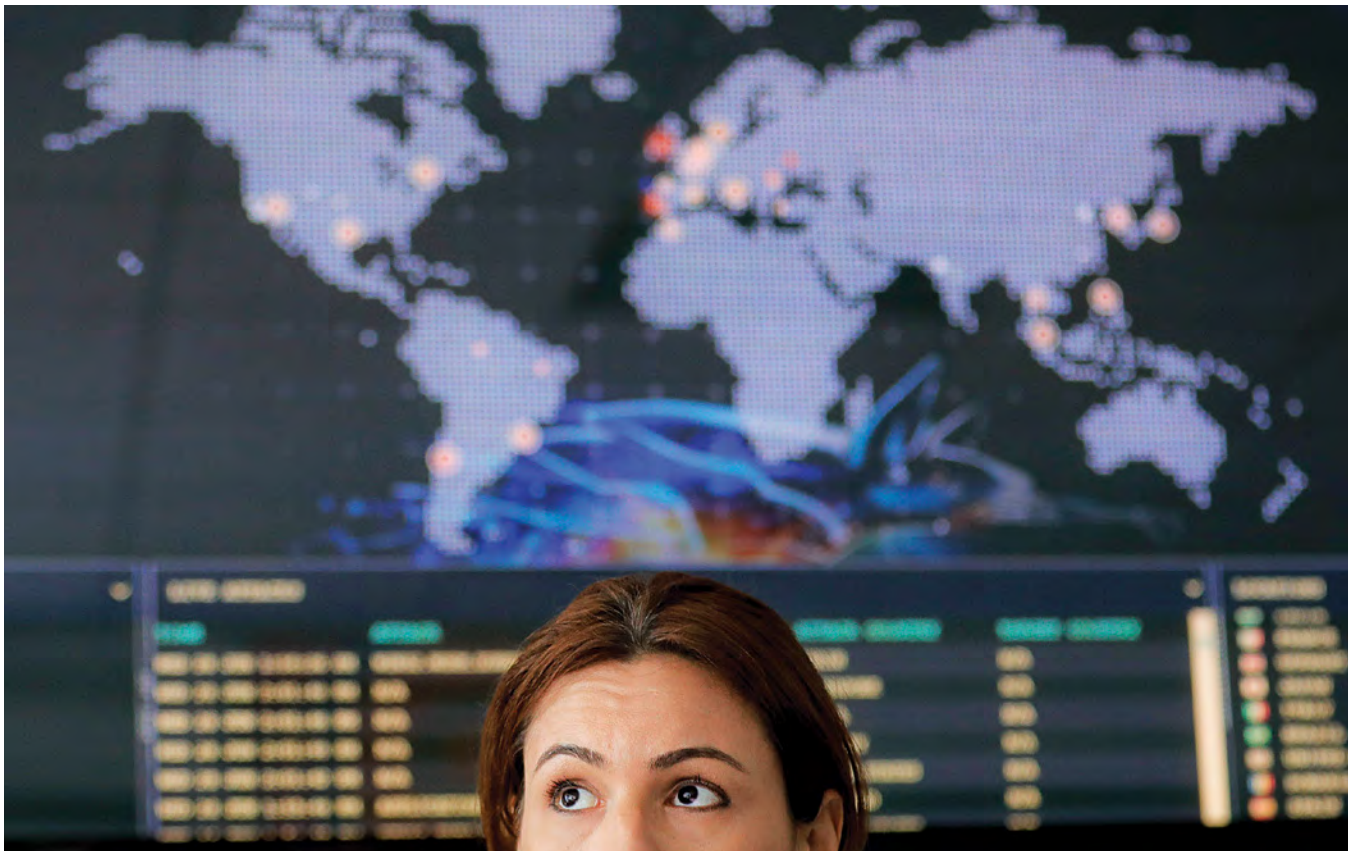
However, techopedia.com provides the following useful definition of cyber defense: "Cyber defense is a computer network defense mechanism which includes response to actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks. 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.

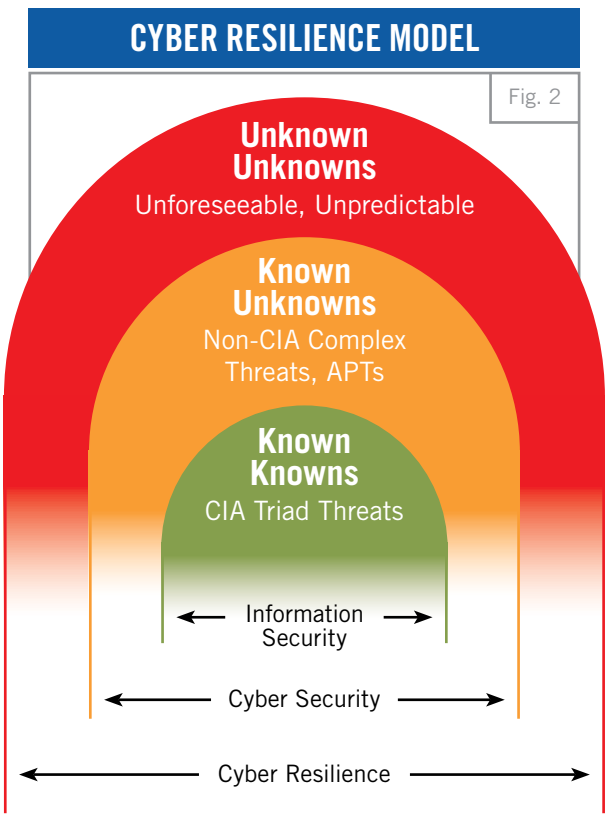
The real cyber security challenge is the unknown. Former U.S. Secretary of Defense Donald Rumsfeld gave this explanation during a news briefing in 2002: "There are known knowns. These are the things that we know. There are known unknowns. That is to say, there are things that we know we don't know. But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