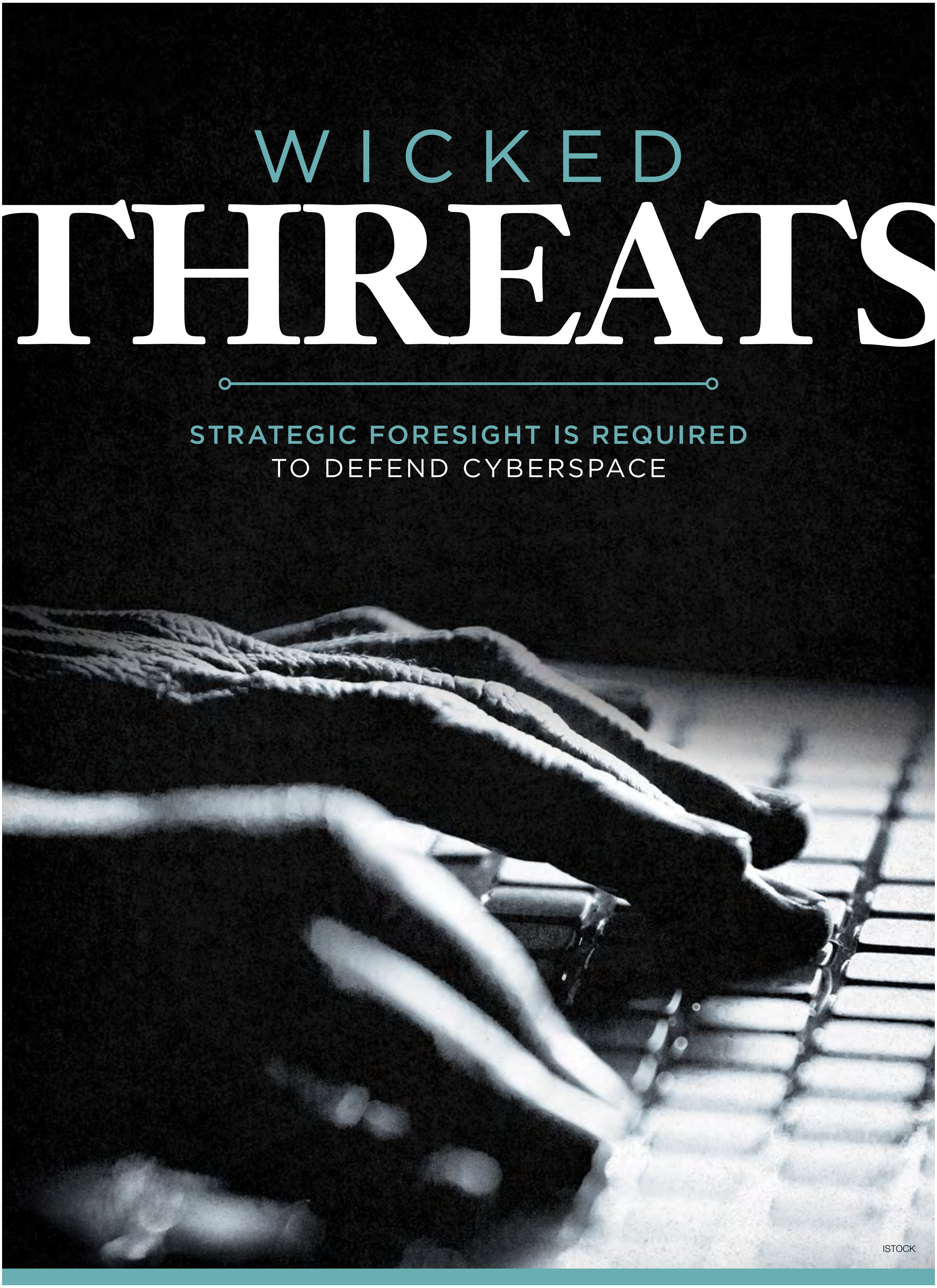
WICKED THREATS

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.

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

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 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.

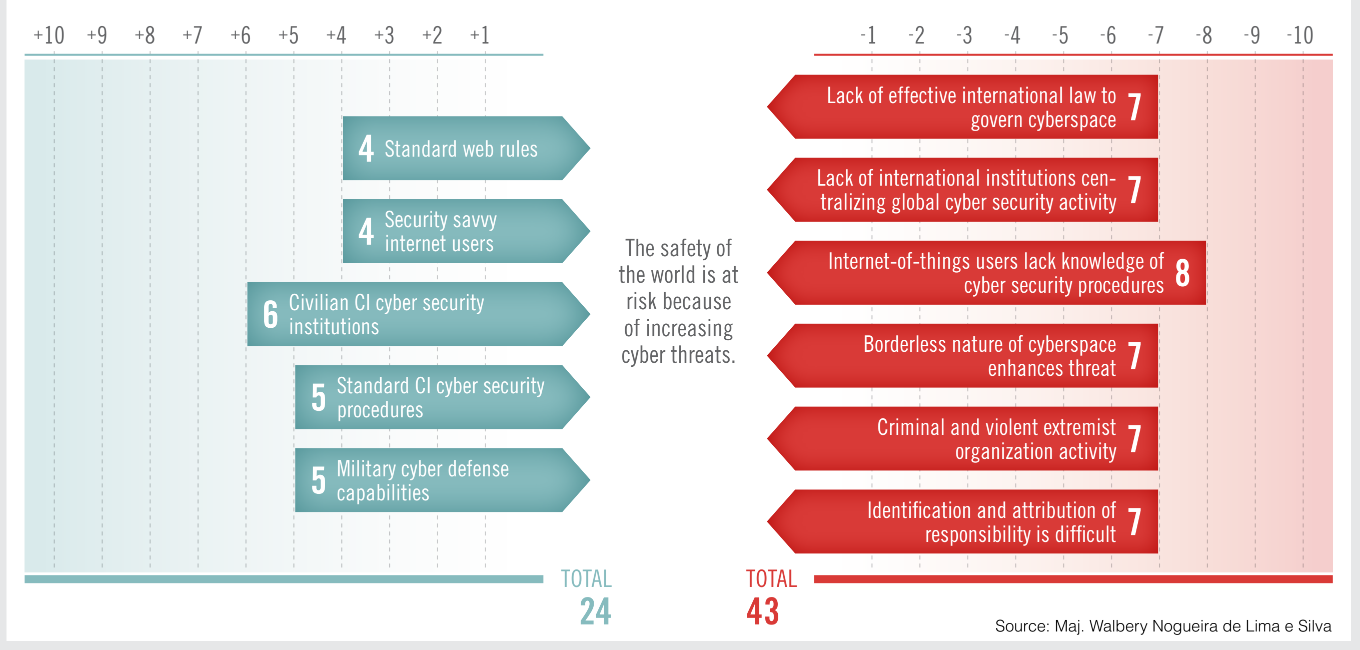
A man uses a 3-D printer during a February 2017 convention of internet users in São Paulo, Brazil. New technologies and the rapidly expanding internet of things require more proactive cyber security measures. REUTERS

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.

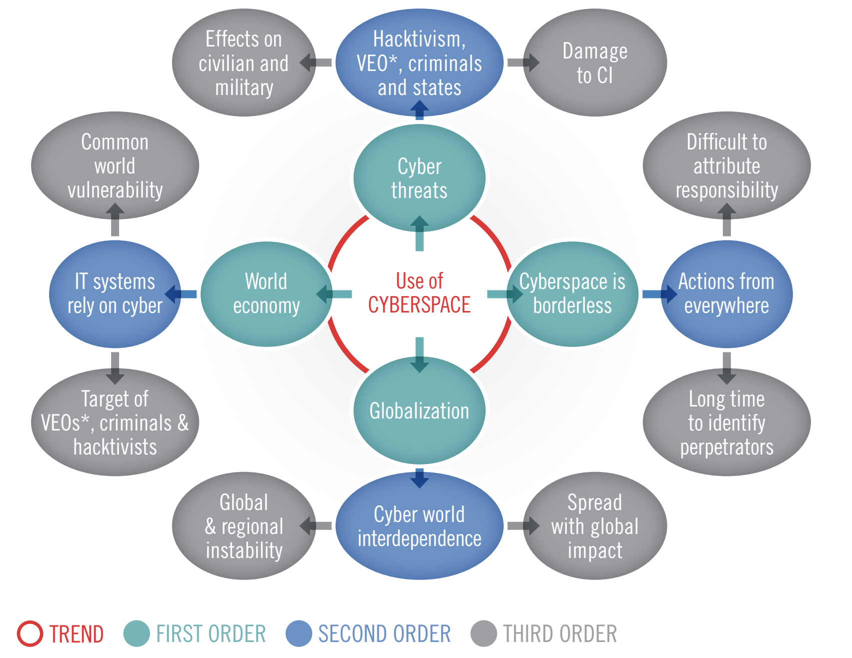
Threats in cyberspace worldwide Force Field Analysis *Fig.* 1



Source: Maj. Walbery Nogueira de Lima e Silva

Futures wheels

Fig. 2

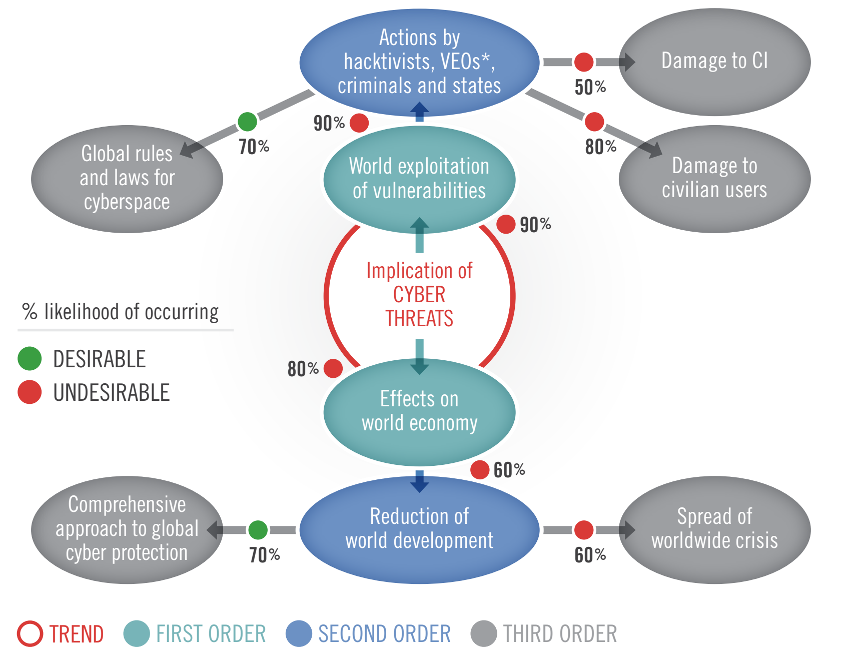

Effects on civilian and military
Hacktivism, VEO*, criminals and states
Damage to CI
Common world vulnerability
Cyber threats
Difficult to attribute responsibility
IT systems rely on cyber
World economy
Use of CYBERSPACE
Cyberspace is borderless
Actions from everywhere
Target of VEOs*, criminals & hacktivists
Globalization
Long time to identify perpetrators
Global & regional instability
Cyber world interdependence
Spread with global impact
TREND
FIRST ORDER
SECOND ORDER
THIRD ORDER

* Violent extremist organizations

Source: Maj. Walbery Nogueira de Lima e Silva

Implication Tree

Fig. 3


Actions by hacktivists, VEOs*, criminals and states
50%
Damage to CI
90%
70%
80%
Global rules and laws for cyberspace
World exploitation of vulnerabilities
Damage to civilian users
90%
Implication of CYBER THREATS
% likelihood of occurring
DESIRABLE
UNDESIRABLE
80%
Effects on world economy
60%
Comprehensive approach to global cyber protection
Reduction of world development
Spread of worldwide crisis
70%
60%
TREND
FIRST ORDER
SECOND ORDER
THIRD ORDER

* 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. □