Effectively Integrating Cybersecurity into National and Economic Security to Improve Outcomes in Both Spheres

Ms. Barbara A. Grewe
Senior Principal, International Strategy and Policy, The MITRE Corporation

**This paper is derived from a presentation the author gave at a NEXT Alliance Conference workshop on November 5-6, 2022, in Annapolis, MD.*

Introduction

Governments routinely pour millions of their financial resources into protecting the national and economic security of their countries and their citizens. Indeed, protecting their citizens' security is one of the essential rationales for government at all. Yet we are increasingly seeing that these essential security efforts are being undermined by a third security domain – cybersecurity. As numerous cyber-related incidents clearly demonstrate, the failure to prevent, adequately respond to, or recover from cyber incidents may render national and economic security measures irrelevant.

Perhaps it is helpful to understand what we mean when we refer to national and economic security. National security has traditionally been viewed principally through a protection lens. The United

States' Code of Federal Regulations, for example, defines national security as referring to "those activities which are directly concerned with the foreign relations of the United States, or protection of the Nation from internal subversion, foreign aggression, or terrorism."[1] Others describe it as an ability of a state to protect and defend its citizens from military and non-military threats, including the "the preservation of the norms, rules, institutions and values of society".[2]

In contrast, economic security is less well-defined. Many, for example, define economic security as pertaining to micro-level concerns such as "the ability of individuals, households and communities to meet their basic and essential needs sustainably; including food, shelter, clothing, health care, education information, livelihoods, and social protection."[3] But increasingly economic security is viewed at the national level to mean "having secure and resilient domestic production capacity, combined with reliable access to the global resources necessary to maintain an acceptable standard of living and to protect core national values."[4]

This latter language hints at the significant overlap between the concepts of national security and economic security. Indeed, this is even more evident in the recently released US National Security Strategy that directly asserts that economic issues "are at the very core of national security and international security and must be treated as such."[5] Japan has similarly recognized the merging of these two types of security in the passing of the Act on Promotion of Ensuring Security by Taking Economic Measures in an Integrated Manner on May 11, 2022, which calls for " the promotion of national security through integrated economic measures."[6]

As such, we are increasingly moving from independent concepts to integrated ones that cannot be considered or addressed in an uncoordinated manner. National security and economic security must be treated in a manner that equally promotes each in the furtherance of the other.

---

[1] 5 CFR §1400.102 (a)(3)

[2] Makinda, Samuel M. Sovereignty and Global Security, Security Dialogue, 1998, Sage Publications, Vol. 29(3) 29: 281-292, cited in Osisanya, Segun, National Security Versus Global Security, The UN Chronicle, www.un.org/en/chronicle/article/national-security-versus-global-security, accessed October 30, 2022.

[3] Global Social Development Innovations, University of North Carolina, at www.gsdi.unc.edu/our-work/economic-security.

[4] 6 U.S.C. § 474(c)(2).

[5] United States, National Security Strategy, October 2022, at 6.

[6] Itabashi, et. al., "Japan: New Act on the promotion of Japan's Economic security enacted", Global Compliance News, July 10, 2022, available at https://www.globalcompliancenews.com/2022/07/10/new-act-on-the-promotion-of-japans-economic-security-enacted240622/

Overarching importance of cybersecurity

Thus, issues of global supply chains for everything from semiconductors to vaccines to aircraft and beyond and the protection of the intellectual property behind these goods cannot be viewed in a vacuum. Nor can they be viewed from a single nation's perspective. These are global issues that transcend borders and are defining elements of the global security landscape.

But if this overlap was not enough, we have a third type of security that is essential to the success of these two other security concepts – which is cybersecurity. What do we mean when we say cybersecurity? According to the US Cybersecurity and Infrastructure Security Agency, cybersecurity refers to "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information." And cybersecurity risk in turn refers to the possibility of physical, financial, or reputational damage due to the failure of ICT systems or cyber physical systems to protect the confidentiality, integrity, or availability of data of the systems or the data contained in them.

The Interrelationship of Economic and National Security with Cybersecurity

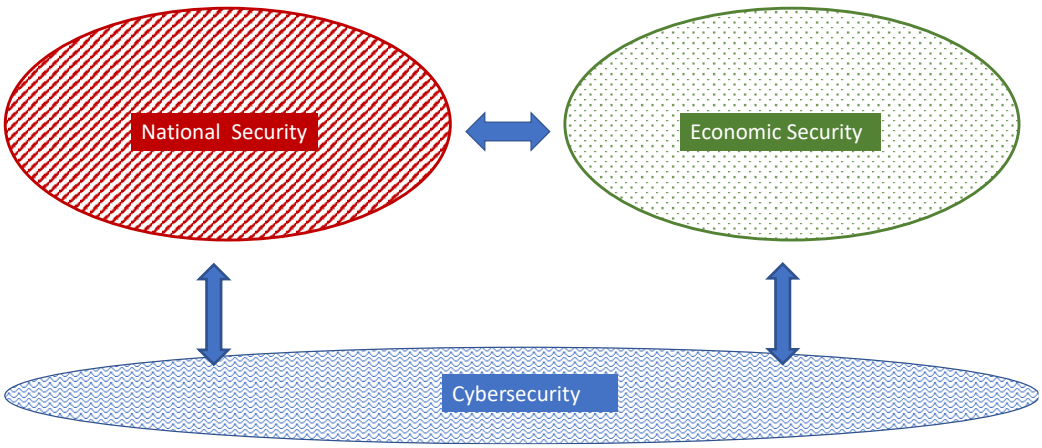

Fig. 1

It is therefore not difficult to determine that effective cybersecurity is essential to maintaining both economic and national security. All types of security rely on data. The loss of confidentiality of the data (meaning adversaries have access to information they should not have access to such as defense plans or intellectual property) or the integrity of the data (meaning that the data can no longer be relied upon as accurate such as activities of adversaries or economic data) or availability

of the data (meaning you cannot access critical data when it is needed) means that your economic and national security may be significantly degraded.

For example, ransomware attacks against critical infrastructure operators or producers of defense equipment or others in the bio-industrial base, can cause significant interruptions to protective operations or critical supply chains. For example, the Colonial Pipeline attack in May 2021 caused supply outages for several days. In 2011, Japan's largest weapons maker, Mitsubishi Heavy Industries, was the victim of a ransomware attack. Malware attacks can steal key information or disrupt critical infrastructure operations. The more recent Russian cyberattacks against Ukraine's critical infrastructure networks were intended to destroy both the national and economic security of Ukraine. Examples abound, such as the breach of the US Office of Personal Management database which had the potential for disclosing the identities of key intelligence assets.

The convergence of cyber and physical security means that no aspect of operations is immune from cyber threats. Distributed Denial of Services (DDOS) attacks can interrupt critical operations. As the Internet of Things becomes ubiquitous and all of the various systems become connected, the potential attack surface broadens exponentially, and the ability to cause damage to one system accessed through a weak link increases vulnerability in another – unless all systems are protected equally. As of 2016, the number of cyber-attacks on Japan's critical infrastructure operators had reached 128 billion.[7] The numbers have continued to increase exponentially.

Indeed, the digital space has routinely been referred to as the new battleground. Traditionally conflicts have been waged on land, sea, or air. Today devastating attacks can be accomplished with a few strokes on the keyboard. Unlike usual kinetic attacks, cyber-attacks may not be visible for months or even years after the attack has taken place and the damage has already been inflicted. Attacks on critical systems do not require physical presence in the country, so traditional border controls are ineffective. New technologies such as drones and widespread use of driverless vehicles will produce new types of threats not previously addressed. The key aspect of these vulnerabilities is that they are introduced through actors over which the government has no control

[7] Naveen Goud, et al. "Cyber Attacks on Japan's Critical Infrastructure Touches 128 Billion Mark." *Cybersecurity Insiders*, 6 Feb. 2017, https://www.cybersecurity-insiders.com/cyber-attacks-on-japans-critical-infrastructure-touches-128-billion-mark/

and very little, if any, influence. Managing such vulnerabilities is further complicated by the larger and more diverse supply chain that our respective governments must rely upon.

There can be no doubt that the security landscape has rapidly evolved and continues to shapeshift as our adversaries seek to stay ahead of our defenses. The National Commission on Terrorist Attacks Upon the United States considered national security in the context of terrorism, noting that traditional national security used to driven by the thoughtful studying of enemies as threats emerged slowly and often visibly. But it concluded that, in contrast, terrorism threats can emerge quickly and from nontraditional sources.[8] This finding is even more applicable in relation to cyber threats as attacks can arise from a vast array of enemies located anywhere in the world and hit the target almost instantaneously.

As a result, cybersecurity cannot be an afterthought to any efforts to address economic or national security. Weak cyber defenses can create devastating national and economic security vulnerabilities and in turn have catastrophic consequences. Cybersecurity must be front and center when deciding how to build national and economic security strategies and implementing them.

This is not a new concept. As Japan's first cybersecurity strategy, issued in 2015, recognized, "cyberspace is increasingly integrated with the real world", and "cyber-attacks have become capable of causing tremendous damages to a state's politics, society, economy, and culture. Nowadays, cyberspace is a sphere not only of economic activities but also of national security and intelligence activities. Disruptive activities, theft of classified information and alteration of data by organized, well-prepared, and advanced cyber-attacks, including those that might be state sponsored, are actual threats today."[9]

The obvious nature of cybersecurity being an essential component of the other security functions that rely on IT systems and the data contained within them is evident in the recent US National Security Strategy which explicitly identifies securing cyberspace as an element of national security.[10]

[8] The National Commission on Terrorism Attacks Upon the United States, Final Report, 2004, at 362.

[9] Government of Japan, Cybersecurity Strategy, September 4, 2015, at 26.

[10] United States, National Security Strategy, October 2022, at 34.

But no strategy or government plan is self-executing. Effective integration of cybersecurity to support the economic and national security realms requires meaningful actions to strengthen our cybersecurity capabilities which in turn requires leadership, increased coordination (both within our respective governments and across international boundaries), and sufficient funding. Weak cybersecurity has the ability to pose an existential threat to national and economic security of our respective countries. Such threats require immediate and comprehensive actions to disrupt the relentless actions of our adversaries.

Recommendations

1. Build strong cyber risk management programs to address the evolving risk landscape

Cyber risk is a function of threats, vulnerabilities, likelihood, and consequences. The cyber risks faced by each nation are too big and too diverse to be completely contained and there can never be enough resources to effectively manage them. Thus, any cybersecurity effort must focus on ensuring that the most important assets are adequately protected. This means prioritizing which risks to address and how to do so.

2. Ensure that structures are erected to permit cross-agency action and responsibility

Too often cyber responsibilities reside in silos. Different agencies create different approaches to the problems, fail to share critical knowledge, and unnecessarily duplicate efforts. Cyber attackers do not respect boundaries of any kind, whether within a government or across governments. Therefore, effective response capabilities should not be hampered by these artificial boundaries. Cross-agency authorities are needed to break down silos. Moreover, there must be ways for to ensure that cybersecurity efforts are fully integrated into the national and economic security apparatuses.

3. Build robust international partnerships

The number and types of relevant stakeholders in the cyber risk arena require new and stronger partnerships to address the ever-expanding risk environment. Partnerships cannot be limited to just government to government. There needs to be public private partnerships. Non-governmental organizations must be part of the effort. The table needs to be made larger to ensure all the relevant stakeholders have a place at it. And because the threat crosses borders with impunity, effective deterrence, mitigation, and/or response requires the allies to join forces.

4. Improve information sharing

Effective cybersecurity initiatives need to accelerate and enhance information sharing regarding cyber threat intelligence and possible vulnerabilities. There is little time between when a new type of attack is discovered and begins to spread. But there is time for effective action if information is shared in real time and effective warning of new threats, relevant indicators, and the tactics, techniques, and procedures used on these attacks is made. This also requires that trusted platforms for sharing are developed, and trusted individuals are designated to receive the information. This may require creating broader and more comprehensive vetting programs for personnel, including national security clearance processes to remove any remaining barriers to effectively and timely sharing.

5. Build cybersecurity "armies" through education and training

Every country complains that it does not have enough cybersecurity professionals to meet mission requirements. Thus, it is essential that partners share education and training opportunities to ensure that new cadres of cyber warriors are produced as quickly as possible. Partners must also be able to leverage the capabilities of trusted partners to broaden the impact of efforts.

6. Improve incident response capabilities

It is clear that no matter how large your army or how effective your information sharing has become, there will be successful cyber-attacks. This means that incident response capabilities have to be in place to ensure that attacks are stopped quickly and effectively to minimize potential damage. Such capabilities require a combination of individuals who can quickly identify the nature of the attack and know how to stop it from spreading. This also requires them to have the necessary authorities and clear responsibilities to ensure the response is not impeded.

7. Create resiliency

In addition to an effective response capability, organizations need to be able to recover quickly and restore operations to pre-attack levels. Building in resiliency is essential to minimizing the impact of any successful attack.

Conclusion

The digital world does not recognize borders – either physical or technological. The fact is that all security domains, including economic and national, rely on similar digital technologies. Thus, cyber vulnerabilities in the economic, food supply, financial, energy, and transportation sectors implicate cybersecurity across all domains. Therefore, no effort should be spared in creating a safe, secure, and resilient digital environment. The future of our countries depends on it.

Ms. Barbara Grewe wrote in her own personal capacity. The views and interpretations expressed by the author are solely her own.

---

*The **US-Japan NEXT Alliance Initiative** is a forum for bilateral dialogue, networking, and the development of joint recommendations involving a wide range of policy and technical specialists (in and out of government) to stimulate new alliance connections across foreign, security, and technology policy areas. Established by Sasakawa Peace Foundation USA with support from the Nippon Foundation, the goal is to help improve the alliance and how it serves shared interests, preparing it for emerging challenges within an increasingly complex and dynamic geostrategic environment. Launched in 2021, the Initiative includes two overlapping lines of effort: 1) Foreign & Security Policy, and 2) Technology & Innovation Connections. The Initiative is led by Sr. Director Jim Schoff.*
