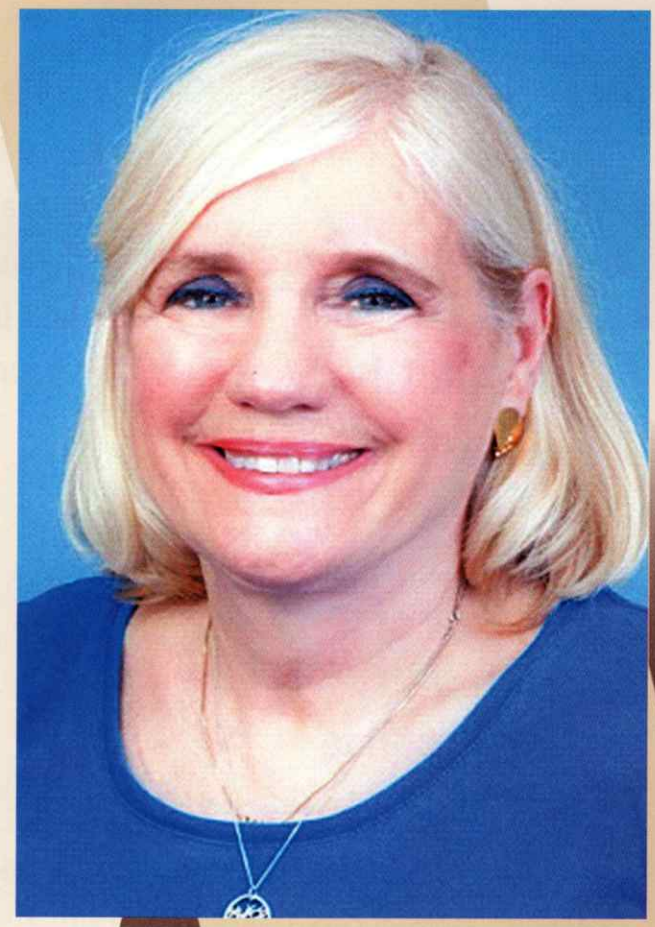
The Role of National Cyber Strategies in Cyberspace Security



by VIRGINIA A. GREIMAN
Senior Advisor, Centre for Strategic Cyberspace + International Studies (CSCIS)

Cyber strategies are a critical force in establishing mandates for our evolving cybersecurity ecosystem. The World Economic Forum's 2018 Global Risks Report ranks both large-scale cyberattacks and major data breaches or fraud among the top five most likely risks in the next decade. Though initial cyber strategies were more aspirational, in recent years these strategies are providing more secure frameworks for national cyber agendas and legal and ethical responsibilities.

Over the past 10 years, national governments have been developing strategies to address emerging security threats associated with the rapidly expanding use of the Internet global network, artificial intelligence and related technologies. These threats have developed into significant national-level problems that include balancing the needs of national security, corporate competitiveness, and privacy protection. Control over national security, criminal conduct, critical infrastructures, global financial services, competitive strategy, medical records, international trade, intellectual property, privacy and a host of other important rights and responsibilities is governed by a paradigm that is conducted in the virtual world. Cyber activity has introduced a whole new meaning to "globalism." Figure 1 illustrates the challenges that governments face in adopting these strategies based on balancing the needs of the national cyber infrastructure system.

What is a Cyber Strategy?

A national cyber strategy outlines a vision and articulates priorities, principles, and approaches to understanding and managing cyber risks at the national level. Failure to prioritize cybersecurity by both government and industry leave nations less secure. Cybersecurity strategies vary by country and represent different interests from a focus on protecting critical infrastructure to improving national intelligence and defense. Cyber threats include cyber warfare, economic and corporate espionage, terrorism and cybercrime.

Strategies require hard choices. The goals of cyber security strategies vary widely as do the methods for implementation. They include: the governance of big data and societal Interest, attack and response theory, standards for government agencies, resilience (strengthening protection), international partnerships, research and development, and institutional reform. Cyber security is just one pillar of most national cyber strategies.

Until relatively recently, the term 'national security' was largely used only within the United States. The widespread introduction of dedicated 'national security strategies' (NSS) in a number of OECD countries is a relatively recent phenomenon that appears to

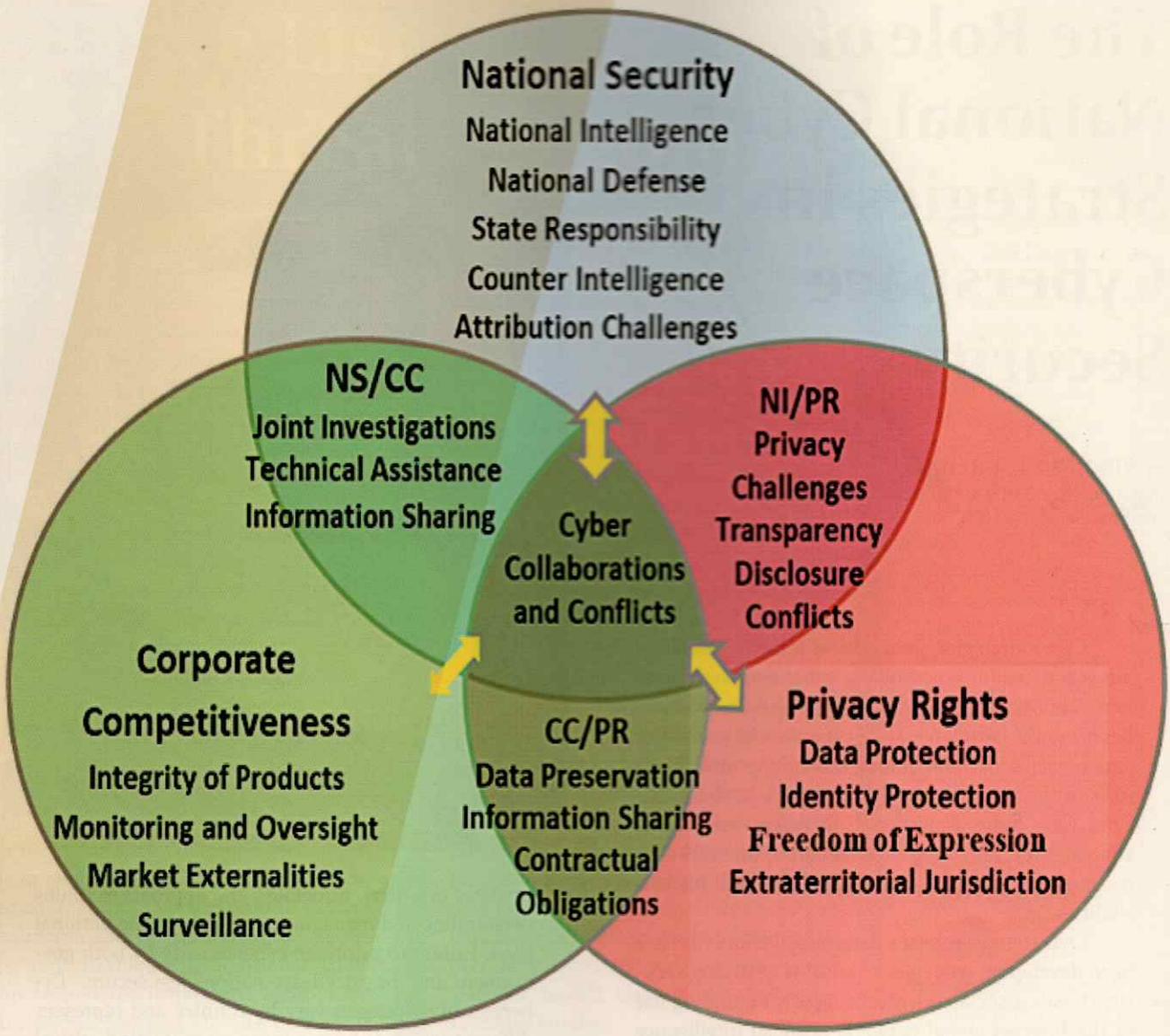


Figure 1: The Cyber Triumvirate
Source: Greiman, V.A. (2016) National Intelligence, Corporate Competitiveness and Privacy Rights: Co-existing in Cyberspace, The Global Studies Journal, Vol. 9 (3), 43-56, September.

have been closely tied to a shift in strategic thought away from focusing on a few specific 'threats' to the idea of mitigation against myriad 'risks'. The growing number and intensity of cyber-attacks requires a closer look at national cyber strategies.

States in all regions of the world now have cyber strategies, reflecting regional mandates (particularly in Europe), multilateral and bilateral discussions, or efforts at assistance in developing national programs. However, as recognized by the European Network for Cyber Security (ENISA), negotiating a multinational agreement involving cyber security will be more difficult due to different perspectives among States. These differences include regulation of content, standards of proof, the extent of extraterritorial investigation, the scope of privacy and the restriction on economic growth by limiting the control exercised by the private sector over the Internet. The lack of common understanding and approaches between countries may hamper international cooperation, the need for which is acknowledged by all countries.

While national strategies may be led by governments, the development of information sharing, policy development, and risk management must be led

by the private sector as they are the primary owners and operators of our cyber systems. The PricewaterhouseCoopers (PwC) 2018 Global State of Information Security Survey of 9,000 business leaders from 122 countries reported that only 31 percent of boards participate in the review of current security and privacy risks, and only 44 percent are involved in setting overall security strategy. Cyber security requires a much more cohesive approach to policy making and organizational governance, not only within the government but within the private sector as well. However, in order for the private sector to understand its role in protecting the nation's infrastructure, cyber strategy must begin at the national level. Legal frameworks should be based upon a principled national strategy that sets a clear direction to establish and improve cybersecurity for government, academia, research and development, business enterprises, consumers, and the technology companies who serve those communities, and society at large. This approach has been advanced by Microsoft and supported by other multinational technology companies. National strategies should include international standards such as ISO/IEC standards on vulnerability and national standards such as the NIST standards used in the United States, and individual protections against privacy breaches, discriminatory treatment, and Internet access.

Characteristics of National Cybersecurity Strategies

Contrasting the cybersecurity strategies of the United States, Asia, and the European Union reveals the following common goals all of which are important goals every strategy should include: (1) develop cyber defense policies and capabilities; (2) achieve cyber resilience; (3) reduce cybercrime; (4) support industry on cybersecurity; (5) secure critical information infrastructures; (6) develop the industrial and technological resources for cybersecurity; and (7) contribute to the establishment of an international cyberspace policy. The recognition that the private sector plays an overriding role in cyber security has created a provision in some recent strategies for incentives for the private sector to invest in security measures.

The level of maturity of national cybersecurity strategies varies widely with some States having developed more sophisticated cybersecurity governance structures, while others are still in the planning phases without metrics, standards or methodologies for assessing their efficiencies. Moreover, most strategies do not include what they consider to be a serious threat that might amount to cyber warfare or a terrorist attack, or how existing strategies can cope with rapidly changing threat dynamics. Nor do national strategies discuss the policies or legislation that is needed to address and prevent these attacks. For instance, South Africa's National Cybersecurity legal policy framework acknowledges that the South African Cybersecurity legal framework will not be a homogeneous document but a collection of legislations, which when viewed collectively will ensure that South African cyberspace is secure.

Most strategies recognize the significant role of the private sector in securing cyberspace and that policies should be based on public-private partnerships, which may include business, civil society and academia. However, they place variable emphasis on this aspect and few clearly describe how public-private partnerships are developed, who should be involved in the partnership and how they will be managed and controlled. In some state strategies it is merely a concept, while in other strategies it is a key pillar.

Selected Cyber Security Strategies

The EU Cybersecurity Act came into force on 27th June 2019. The Cybersecurity Act aims to achieve a high level of cybersecurity and cyber resilience, and to promote individuals' trust in the EU digital single market. The Cybersecurity Act aims to reinforce ENISA's role as the EU's center of advice and expertise with regard to cybersecurity matters and to facilitate the development and implementation of EU policy and law. The Act introduces a voluntary, centralized cybersecurity certification framework, thereby avoiding a splintered approach by Member States adopting their own separate standards.

In the United States, strengthening cybersecurity capabilities by bolstering cyber defence and cyber deterrence are two of the country's highest priorities. The 2018 U.S. National Cyber Strategy promotes four pillars: Defend the homeland by protecting networks, systems, functions, and data; (2) Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation; (3) Preserve peace and security by strengthening the ability of the United States — in concert with allies and partners — to deter and, if necessary, punish those who use cyber tools for malicious purposes; and (4) Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet.

The government in Japan has updated its strategy every few years since the first one was released in 2013. The WannaCry ransomware attack in May 2017

in Japan that infected 2,000 computers at 600 organizations may have increased the urgency for moving forward with its new strategy. Japan's newest strategy published in 2018 aims to improve the cybersecurity of Japanese critical infrastructure and encourage Japanese businesses to pursue cybersecurity best practices, both of which will help Japan's economic growth and innovation. A focus on improving cybersecurity in the private sector is central to the new strategy.

In December 2016 the Cyberspace Administration of China (CAC) released its National Cybersecurity Strategy which illustrates and reaffirms China's main positions on cyberspace development and security. The Strategy aims to build China into a cyber power while promoting an orderly, secure, and open cyberspace and safeguarding national sovereignty. The Strategy addresses cybersecurity as "the nation's new territory for sovereignty" and marks a new step in streamlining cyber control. Its major objectives are in alignment with the key cyber strategies of other countries including the protection of national security, defending cyberspace sovereignty, protecting critical infrastructure, fighting cybercrime, and strengthening international cooperation.

International Strategies

It is not sufficient today to just focus on national strategies. If we are to defeat the global threats of cybercrime, cyber terrorism and economic espionage we must have global partners to assist in combatting and responding to these threats. Though national strategies are evolving rapidly, and many stress the importance of the international dimension of cybersecurity and the need for better alliances and partnerships with likeminded countries or allies, including capacity building of less developed countries, clearly articulated international strategies for cyberspace are still in the early stages of development.

Partnerships already exist with many international organizations on cyber infrastructure and security-including the International Criminal Police Organization (INTERPOL), the United Nations, the G-8 alliance, NATO, the Council of Europe, the Asia-Pacific Economic Cooperation forum, the Organization for Economic Cooperation and Development (OECD), the International Telecommunications Union (ITU), the European Council on Cybercrime, and the International Organization for Standardization (ISO). The Group of Eight (G-8) and private groups such as the Internet Alliance have issued guidelines aimed at making voluntary cooperation more effective. Although these groups recognize that international cooperation is essential, they have yet to accept that an international treaty establishing legally mandated standards and obligations should be negotiated.

As argued by scholars and policymakers there exists a strong case for a legally mandated, international regime to advance agreement on codes of conduct, norms, and international treaties. Some scholars have suggested the establishment of an international agency, modeled along the lines of specialized United Nations agencies, to prepare and promulgate— on the basis of advice from nonpolitical experts—standards and recommended practices to enhance the effectiveness of protective and investigative measures.

SUMMARY

Nations depend on cyberspace for the gathering of national intelligence, increasing corporate competitiveness, improving the economy and the quality of life of all its citizens. Thus, reducing the risks of cyberspace is critical to a nation's prosperity. Conflicting goals and challenges have emerged from the overlapping interests and responsibilities of the various actors in cyberspace. The resulting triumvirate of national interests, privacy and global competitiveness is now far more complex than each of the individual issues and dominates much of the discourse about cybersecurity. Prioritizing these interests creates conflicts that result in competing concerns that cannot be easily reconciled. It also raises the importance of the need for collaboration and partnering to resolve universal problems and the need for better national intelligence and defense. A global legal framework that balances national and private interests would enhance confidence and improve legal certainty in the global electronic marketplace. As national cybersecurity strategies continue to evolve it will be essential to identify the commonalities among these strategies so that a model for harmonizing the shared interests of all nations in a peaceful and secure world can be developed and implemented.