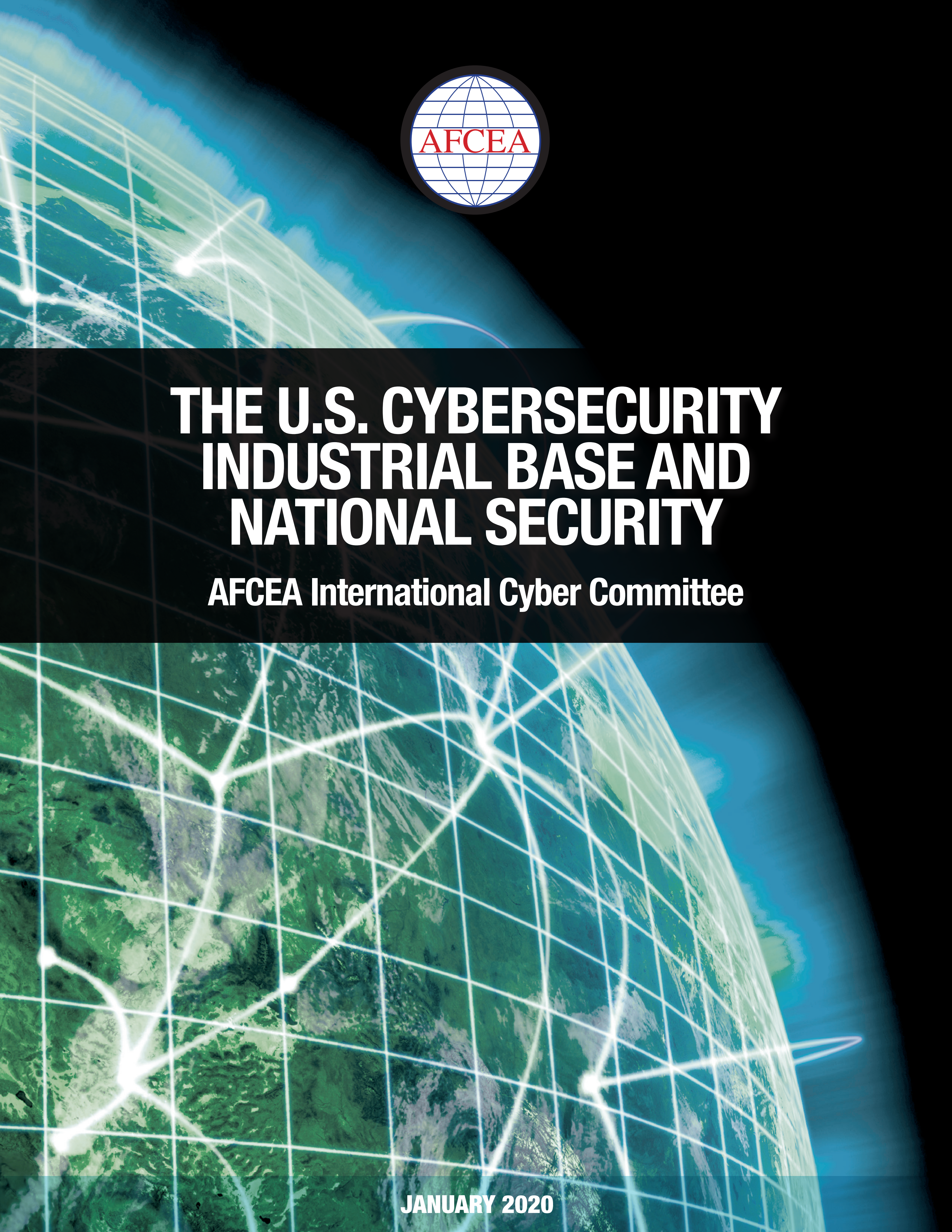


THE U.S. CYBERSECURITY INDUSTRIAL BASE AND NATIONAL SECURITY

AFCEA International Cyber Committee

JANUARY 2020

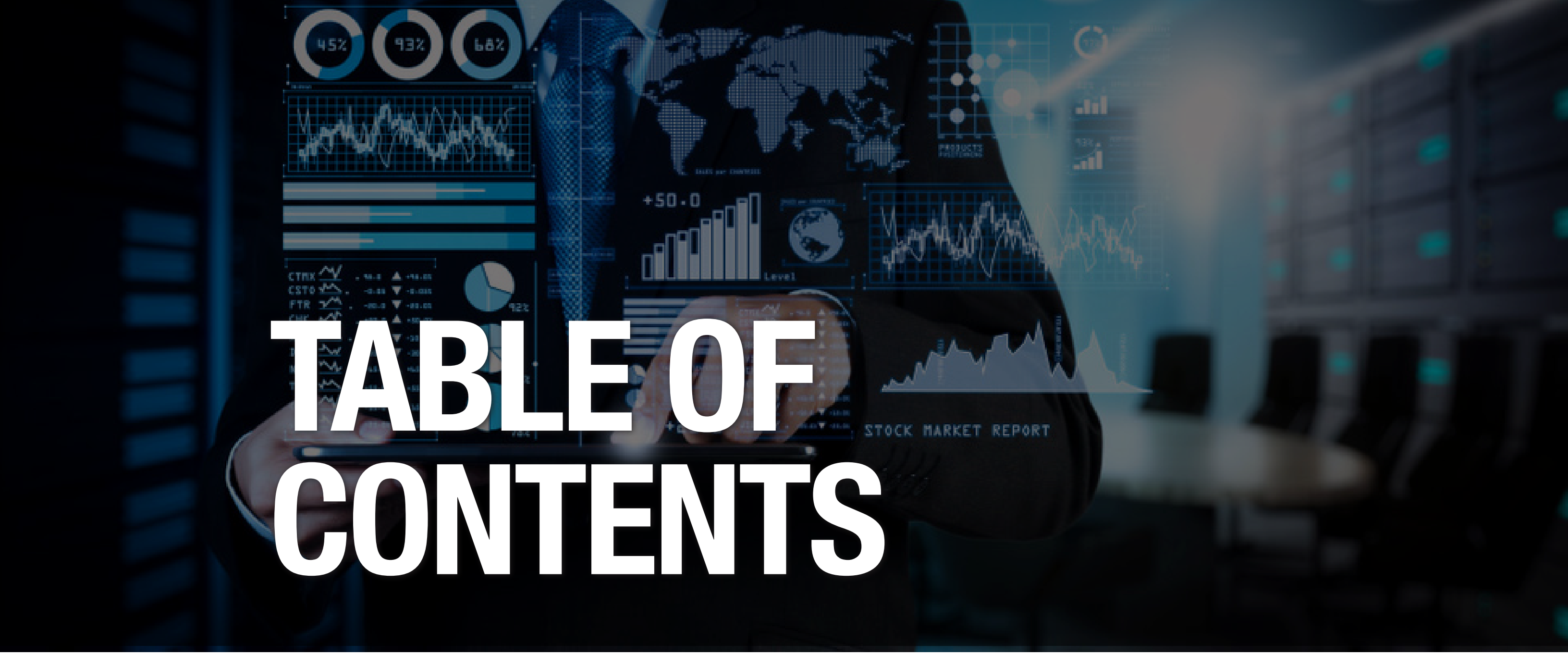


TABLE OF CONTENTS

Introduction and Executive Summary 3

The State of the Industrial Base 4

Challenges Persist 5

"Houston, We Have a Problem" 7

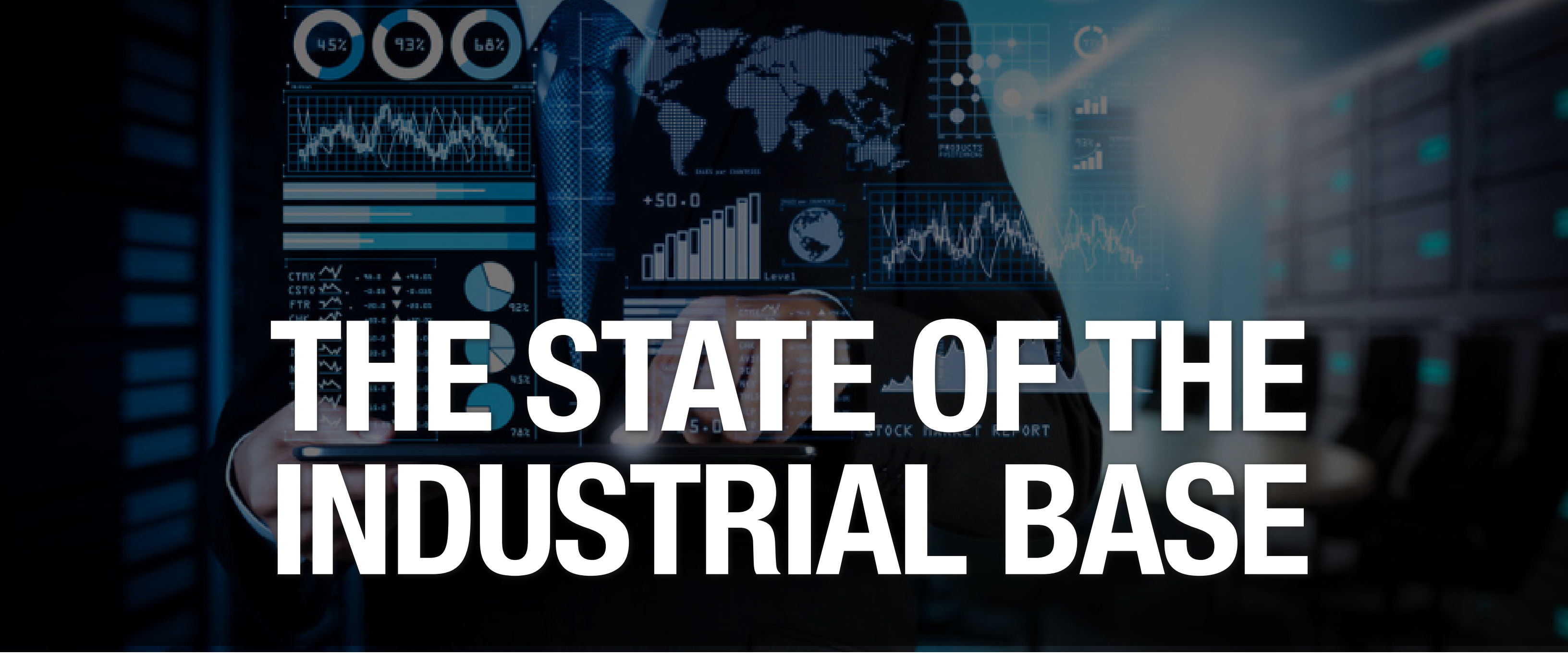
Recommendations Moving Forward 8

Conclusion 10

References 11

INTRODUCTION AND EXECUTIVE SUMMARY

This white paper conveys to U.S. national security policy makers and decision makers observations and recommendations regarding the nation's cybersecurity industrial base and this sector's ability to support and strengthen the national security of the United States. While this paper does not encompass an exhaustive survey of the nation's current cybersecurity industrial base, it does provide a summary of observations regarding the state of that industrial base as it relates to current and prospective national security needs.



THE STATE OF THE INDUSTRIAL BASE

In general, committee members view the state of the U.S. cybersecurity industrial base as robust. Among the companies are numerous start-ups exploring new and in some cases pioneering cybersecurity technologies as well as cybersecurity service providers, consultancies, security service providers and product manufacturers.

The cybersecurity market in the United States and globally continues to grow briskly, mirroring rising demand. With a global market of almost a quarter of a trillion dollars by 2025 and a U.S. market of almost $100 billion by that same year, the cybersecurity market remains richly resourced. Analysts[1] expect a compound annual growth rate of 11 percent between now and 2025, outpacing most other economic sectors.

The U.S. cybersecurity industrial base benefits from an infusion of cybersecurity technologies and innovations originating in friendly countries as well as allies, including Israel, the United Kingdom and Australia. The aggregate demand for cybersecurity services and products throughout Five Eyes partners, NATO members and Israel creates a larger market for innovation, thus enriching the range of technologies available to the United States. Overall, vigorous competition exists for cybersecurity products such as endpoint security, firewalls, intrusion detection and protection systems, anti-virus tools, anomalous behavior detection tools, managed security services and security consulting.

CHALLENGES PERSIST

However, significant questions persist, and it is not clear the U.S. cybersecurity industrial base is positioned to address these challenges effectively, including:

- Potential breakthroughs in decryption, including quantum computing.
- The use by adversaries of artificial intelligence (AI) to probe, find and exploit vulnerabilities in U.S. systems, and the use of AI to create custom exploits against specific vulnerabilities.
- The potential vulnerabilities associated with complex infrastructures, including “smart cities” that employ AI-based analytics to mediate resources such as transportation, energy, water and policing.[2]
- Global 5G wireless deployment on which U.S. interests will depend.
- Commercial satellite constellations that will serve U.S. national security and business interests such as constellations that will number in the tens of thousands.
- Commercial cloud computing, cryptography and identity enablement.
- Reports that indicate the companies comprising the Defense Industrial Base remain under constant threat.
- The increased use of ransomware as a weapon, and the difficulties encountered in blocking and defeating ransomware attacks.

Concerning the ransomware conundrum, cybersecurity products can be expensive and difficult to use, impairing the ability of many enterprises to use them effectively. A recent report[3] notes that ransomware payouts in the third quarter of 2019 averaged more than $41,000, a 13 percent increase from the same quarter in 2018. While it is true that resistance to payouts has grown and the rate of increase has stabilized, the persistence of ransomware and the range of sectors it affects—from hospitals to public schools, from energy companies to city governments—increases the need for practical solutions to a menace that continues to reward cyber criminals.

Another development that is perhaps even more troubling involves the energy sector. The nation’s largest solar power operator was hit by a denial-of-service attack that penetrated a known vulnerability, resulting in what the U.S. Department of Energy called “interruptions of electrical system operations.”[4]

While the economic effects of cybercrime are difficult to determine with certainty, a 2018 report[5] by the Center for Strategic and International Studies and McAfee shows that more than three-quarters of a point of the U.S. Gross Domestic Product (GDP) is lost to cybercrime and almost one percent of global GDP is lost to cybercrime.

The effects of adversarial computer network exploits and attacks on the United States extend to every sector, including the election systems, a foundational institution of U.S. democracy. The seeming ability of Russia to conduct information maneuvers to achieve specific outcomes among U.S. voters, to amplify political and social differences, and to undermine institutions has led to the development of a disciplines known as "social cybersecurity," which are described as:

- "[t]he science to characterize, understand and forecast cyber-mediated changes in human behavior, social, cultural and political outcomes, [and]
- "[t]he science and engineering to build the cyber-infrastructure needed for society to persist in its essential character in a cyber-mediated information environment under changing conditions, actual or imminent social cyber-threats."[6]

Despite work done to identify and characterize information maneuvers and other efforts to erode U.S. national interests, adversaries persist in their use, targeting institutions and political moves in the United States, Europe, Ukraine and Asia.

Cyber criminals and foreign governments are clever and adaptive in their use of offensive cyber technology. For example, operations at a major European airport were affected by an infection of crypto-currency mining software that "enslaved" much of the airport's rich computing environment to mine the Monero cryptocurrency.[7]

“HOUSTON, WE HAVE A PROBLEM”

Broadly speaking, the U.S. national cybersecurity industrial base, while economically vigorous, is not yet adequate to protect its national interests. Reasons for this problem include:

- Swift development and adaption by adversaries of cyber exploit and attack tools.
- The growth of large-scale criminal and government cyber operators equipped with advanced technology and the resources, intelligence and tradecraft to undertake persistent operations, leaving targets “outgunned.”
- A lack of consensus regarding important research and development challenges that must be met, coupled with a lack of a whole-of-nation cybersecurity research and development strategy or coordinated R&D community.
- Cybersecurity tools that are seemingly too expensive and difficult to operate for many enterprises.[8]

RECOMMENDATIONS MOVING FORWARD

Meeting these challenges requires real partnership between the nation’s public and private sectors and may require government leadership to help identify technical challenges and ensure that market structures and incentives are adequate to meet these challenges. Such a partnership may represent an example of industrial policy, an approach eschewed generally in the United States.

However, the United States is increasingly dependent on the private sector and critical infrastructures. More importantly, the country’s dependency on the commercial sector’s security systems and an emerging global infrastructure the United States can influence but does not necessarily control makes a robust, purposeful approach necessary. Research resources need to be as robust as possible, giving smaller and medium-size enterprises the benefits not only of effective cybersecurity but also of the nation’s major public and private sector institutions.

The elements of such an approach should include:

- Development of a national cybersecurity R&D community that includes government, industry and academia, as well as consensus on key national cybersecurity R&D challenges and an operational concept by which this community would work on in concert to address those challenges.[9]
- Development of a national cyber range to measure the actual cyber effects of commercial tools, in complex, high-threat environments.
- Establishment of a pedigreed “Good Housekeeping Seal” for cyber tools.
- The increase in more explicit government direction to industry regarding the cybersecurity technologies that would improve a wide range of national industrial and infrastructure sectors.
- Close coordination among the Office of Science Technology and Policy, the Defense Department, the Department of Homeland Security, the Office of the Director of National Intelligence, and the Department of Commerce to identify technology challenges the cybersecurity industrial base should meet.

- Collaborative efforts by government, industry and academia to lower the costs of cybersecurity tools and services, coupled with efforts to improve the usability by defining the capability of these tools and services.
- A move past compliance-based cybersecurity and into more well-defined effects-based cybersecurity.
- A purposeful effort to promote the work of the National Cybersecurity Center of Excellence of the National Institute of Standards and Technology. The center develops reference architectures[10] applicable to a wide range of industry verticals. The architectures consist of commercial cybersecurity products and can be used to buttress the cyber defenses of companies ranging from transportation to energy, from health care to financial services and from retail to hospitality.
- Industry efforts to couple more directly the development of cybersecurity technology to emerging information technologies. The rise of AI mediated enterprises and infrastructures represents a significant challenge to the cybersecurity industry. Such enterprises and infrastructures are complex; their AI analytic engines may be subject to data poisoning; and adversarial behavior may be difficult to detect. In fact, adversaries may use AI to detect and exploit vulnerabilities and even to craft new exploits on the fly in response to transient vulnerabilities.
- Finally, the Office of Science Technology and Policy, Defense Department, Department of Homeland Security, the Office of the Director of National Intelligence and the Department of Commerce should consider an undertaking such as In-Q-Tel[11] to make targeted investments in cybersecurity technologies and products that would address key challenges that can be cost effective, easy to use and brought to market in six to 36 months, reflecting In-Q-Tel's model.

CONCLUSION

The cybersecurity threats to the United States continue to expand, as do the assaults on the country's business and critical infrastructures, government and foundational institutions. Despite a robust cybersecurity industrial base, the United States remains more at risk than in the past and faces adversaries that are increasingly clever and ambitious.

Closing the gaps in the U.S. cybersecurity industrial base represents a difficult challenge but one the United States can meet. Whether the country chooses to call the recommendations above industrial policy or regard them as a coordinated set of initiatives, these ideas represent a starting point for consideration.

Taking action will require leadership and strategy. The AFCEA Cyber Committee offers these recommendations as first steps and stands ready to support a national effort focused on their implementation.

REFERENCES

1 See https://www.grandviewresearch.com/press-release/global-cyber-security-market

2 See https://www.alibabacloud.com/et/city

3 See https://www.govinfosecurity.com/ransomware-average-ransom-payout-increases-to-41000-a-13333

4 See https://www.eenews.net/stories/1061421301

5 See https://www.computerweekly.com/news/252435439/Economic-impact-of-cyber-crime-is-significant-and-rising

6 See https://sites.google.com/view/social-cybersec/

7 See https://www.linkedin.com/company/cyber-defense-magazine/

8 At this writing, the U.S. Department of Defense is encouraging companies that comprise the Defense Industrial Base to adopt the guidelines contained in NIST 800-171, even as smaller companies in the Defense Industrial Base struggle with the economics of doing so.

9 Precedents exists such whole-of-nation R&D strategies, encompassing the World War II effort to develop nuclear weapons, post-WWII efforts to achieve commercial nuclear power and aerospace preeminence, and the remarkable progress made in recent decades against HIV/AIDS.

10 See https://www.nccoe.nist.gov/

11 See https://www.iqt.org/

The AFCEA International Cyber Committee White Paper Series

www.afcea.org/committees/cyber

AFCEA