twosix TECHNOLOGIES

NATIONAL SECURITY IN THE DIGITAL AGE:

LEVERAGING AMERICA'S TECHNICAL ADVANTAGE

National Security in the Digital Age: Leveraging America's Technical Advantage

The digital revolution is a double-edged sword for national security. While innovations in artificial intelligence (AI), biotechnology, quantum computing and other emerging technologies offer powerful tools to combat threats, they also introduce potential risks.

Consequently, the United States finds itself in a period of intense strategic rivalry, with the quest for technological dominance taking center stage. To ensure the nation's security, the intelligence and defense communities must recognize the threats posed by emerging technologies and leverage these same advancements to safeguard the homeland.

In this white paper, we'll explore:

- The top challenges to our national security today
- A strategy for using emerging technologies to mitigate these challenges
- Two Six Technologies products that help make the world safer

Meet the Author

Elizabeth "Beth" Kimber is a veteran of the intelligence community with a 37-year career at the CIA. She served as the Deputy Director of CIA for Operations and as Acting Deputy Director of CIA, where she was the agency's second-in-command. Notably, she also served as the first Assistant Director for Europe and Eurasia, Deputy of the National Clandestine Service, Chief of National Resources Division and spent 18 years in the field, including assignments as chief of station.

In 2022, Beth transitioned to Two Six Technologies, taking on the role of Vice President of Intelligence Community Strategy. In this position, she helps steer the company's growth and solidify its status as a leader in cutting-edge national security technologies.

The Challenges We Face

The threats facing the nation are numerous and constantly evolving, primarily due to the ambitions of our geopolitical rivals and technological developments. Some of the biggest risks today include:

- Emerging disruptive technologies
- Cyber threats and information warfare
- Geopolitical dynamics and conflicts fought in the gray zone
- Data overload and analysis challenges
- AI's dual-use nature
- Competition with China
- Workforce shortages

Emerging Disruptive Technologies

The spread of new technologies such as AI, 5G telecommunications, CRISPR gene editing, quantum computing, and the development of smart cities presents both strategic opportunities and challenges. These technologies can enhance national security but also introduce vulnerabilities and new threats as countries compete for technological supremacy.

EXAMPLE: AI IN PREDICTIVE DEFENSE SYSTEMS

Nations want to use AI to enhance their predictive defense systems capabilities. This is evident in the U.S. military's focus on Combined Joint All-Domain Command and Control (CJADC2) and its emphasis on enhancing interoperability across multiple platforms and armed services.

By integrating AI-driven analytics and machine learning algorithms, CJADC2 allows for real-time processing of vast amounts of data from disparate sources — ranging from satellite imagery to sensor data on the ground. This allows for a cohesive and flexible command and control environment, ensuring that important decisions are backed by detailed, precise, and timely intelligence.

EXAMPLE: AI IN SMART CITIES

Regarding surveillance, countries like China use smart city technologies to enhance their monitoring capabilities. These systems integrate vast networks of sensors and CCTV cameras, all powered by AI, to analyze data in real time. This allows for unprecedented levels of surveillance and is part of a broader strategy to maintain social order and monitor public spaces continuously.

Cyber Threats

Cyberattacks executed by state actors, non-state entities and criminals to disrupt and compromise networks and steal data are impacting national security and resulting in billions of dollars in economic losses.

EXAMPLE: 5G AND THE RISK OF CYBER ESPIONAGE

The United States and several other countries have expressed concerns that Huawei's close ties to the Chinese government could threaten national security. These concerns stem from the possibility that the Chinese government could exploit Huawei's 5G technology to conduct cyber espionage, collect massive amounts of data, and potentially disrupt critical communications networks and public utilities. The U.S. has taken measures such as imposing restrictions on Huawei as part of a broader effort to mitigate these risks.

EXAMPLE: CYBERATTACKS ON POWER GRIDS

In early 2023, a significant attempt was made to sabotage Ukraine's power grid. Russian hackers targeted the grid with the intent of causing a massive blackout affecting approximately two million people. This operation involved malicious software known as a 'wiper,' designed to erase essential operational data and render systems inoperable. However, Ukrainian officials stated they thwarted this attack, preventing what could have been the largest cyber-induced blackout in history.

Geopolitical Dynamics and Conflicts Fought in the Gray Zone

Geopolitical struggles are increasingly fought in an ambiguous space known as the gray zone. Here, states and non-state actors use coercive and aggressive tactics, like cyberattacks on critical national infrastructure and influence campaigns, to achieve their goals without resorting to outright war.

According to a 2019 report by the Oxford Internet Institute, 52 countries used "disinformation and media manipulation" to mislead users, and 47 countries used state-sponsored trolls to attack political opponents or activists. These orchestrated campaigns can skew public perception, undermine trust in democratic processes, and sway election outcomes, effectively manipulating the political landscape without direct physical intervention.

EXAMPLE: SOCIAL MEDIA MANIPULATION IN ELECTION INTERFERENCE

A notable instance of foreign interference in national elections is Russia's meddling in the 2016 United States presidential election. This interference aimed to sow discord and division within the U.S. populace, undermine trust in democratic institutions, and influence the election outcome.

Data Overload and Analysis Challenges

The intelligence community faces challenges in managing, processing, and analyzing the vast amounts of data generated daily. This data deluge can overwhelm existing systems and processes, making it difficult to extract actionable intelligence. There are also interoperability issues as solutions from disparate vendors or sources fail to work harmoniously, introducing friction and even points of failure to the intelligence-gathering process.

EXAMPLE: REAL-TIME SOCIAL MEDIA ANALYSIS DURING CRISIS SITUATIONS

Throughout the Russo-Ukrainian War, Ukraine has been leveraging crowd-sourcing to gather intelligence and evidence against war crimes by involving its citizens directly through various digital platforms. The Ukrainian government has set up several tools, including chatbots like "e-Enemy," that enable citizens to report incidents of war crimes and other violations to the authorities.

This innovative use of crowd-sourcing comes with two significant challenges: verification and data overload. Validating the authenticity and accuracy of this intelligence is a critical, yet resource-intensive process. Plus, the sheer volume of information can overwhelm existing systems, leading to delays in data processing and potentially critical insights being missed.

AI's Dual-Use Nature

While AI offers significant advantages for national security, such as enhancing imagery analysis and decision-making processes, it also poses risks related to data manipulation, bias, and the potential misuse by adversaries to compromise systems and spread disinformation.

EXAMPLE: AI-ENHANCED DEEPFAKES FOR DISINFORMATION CAMPAIGNS

A video surfaced on social media in March 2023 displayed South African President Cyril Ramaphosa announcing controversial changes to address the country's energy crisis. Despite its lack of realism, this "cheap fake" video, which is a less sophisticated form of deepfake, managed to go viral and was believed to be real by some viewers.

Competition with China

One of the most pressing challenges to U.S. national security is the strategic competition with China as outlined in the 2024 Intelligence Community Threat Assessment. The country intends to become the pivotal node in the global AI landscape by 2030. This ambition is backed by heavy state investments and an aggressive policy stance where the country aims to set global standards in AI technologies. This strategic positioning is seen as a direct challenge to U.S. technological leadership and its geopolitical influence.

The report also reiterates longstanding concerns over China's practices regarding intellectual property (IP) theft. This includes sophisticated cyber espionage operations directed toward U.S. industrial sectors and research institutions, which are viewed as integral to China's strategy to leapfrog into leadership positions in high-tech industries. This not only undermines U.S. economic interests but also poses a direct threat to national security by enabling significant advancements in Chinese military capabilities.

EXAMPLE: INTELLECTUAL PROPERTY THEFT IN SEMICONDUCTOR TECHNOLOGY

In 2023, ASML, a leader in the global semiconductor industry, accused a former China-based employee of misappropriating sensitive data from the company. ASML is one of the few companies capable of producing advanced lithography machines essential for manufacturing the sophisticated semiconductors required for advanced military hardware.

Workforce Shortages

The rapid pace of technological change demands a workforce with specialized skills in areas like AI, cybersecurity, and data analytics. However, the pool of talent with the necessary clearances and expertise is not keeping pace with the demand. For the intelligence community in particular, this is a major problem. Highly trained, technical personnel are vital to our national defense, and also to the innovations that power our offensive security strategies. Organizations like the National Security Agency (NSA) recently directed a hefty amount of resources to support a surge in hiring, plus benefits and educational opportunities to close skill gaps.

EXAMPLE: IT TALENT REMAINS IN SHORT SUPPLY

According to Gartner, IT executives identify talent shortage as the biggest hurdle for adopting 64% of emerging technologies. This is a stark increase from just 4% in 2020. The lack of skilled personnel far outweighs other concerns, such as implementation cost (29%) and security risk (7%). This shortage impacts the ability of the government to leverage the newest technologies for both defensive and offensive purposes.

Solutions for Improving America's National Security Profile

In a time marked by swift technological progress and intricate global issues, America's approach to national security is continuously being tested and pushed to adapt. The ideas laid out here aim to enhance existing security protocols and forge new paths by combining the capabilities of the public and private sectors, cutting-edge technologies, and innovative policies. By adopting these methods, the United States can strengthen its defenses, sharpen its intelligence capabilities, and maintain its leadership in global security matters.

Strengthen Public-Private Partnerships

Enhancing the collaboration between the intelligence community and the private sector can go a long way in ensuring our national security. This partnership is vital for sharing critical information, fighting threats, fostering innovation, and creating scalable solutions that can operate both within and across different government agencies and allied nations.

The idea is to bridge the gap between government secrecy and the innovative potential of the private sector to address national security challenges effectively and rapidly at the speed of innovation.

EXAMPLE: DEFENSE INNOVATION UNIT (DIU)

The DIU was established by the Department of Defense (DoD) to facilitate the transfer of cutting-edge technologies from Silicon Valley's tech companies to the military. The initiative aims to make the U.S. armed forces more innovative by integrating commercial technology into military capabilities, thereby addressing national security challenges more effectively.

Embrace New Technologies

The intelligence community must leverage cutting-edge technologies, including AI, machine learning, and quantum computing. Integrating these tools would allow the intelligence community to enhance its capabilities in assessing threats, provide timely warnings, and support decision-making processes.

However, integration is easier said than done due to adoption barriers that include:

- **Rapid Technological Advancement Challenges:** The intelligence community must continuously adapt to the evolving technological landscape, ensuring they stay ahead of adversaries who are also utilizing similar technologies. The pace at which technology evolves demands constant vigilance and flexibility in adoption strategies to maintain a competitive edge.

- **Quantum Computing Challenges:** Quantum computers are extremely sensitive to environmental factors like temperature fluctuations and dust contamination, which can disrupt their operation. Plus, current quantum systems require sophisticated cooling mechanisms to maintain near-absolute zero temperatures to operate effectively, adding to the complexity and cost of these systems.

- **AI Adoption Hurdles:** There is a notable skills gap within the intelligence community for deploying and effectively managing AI technologies, reflecting a broader challenge across various sectors. Incorporating AI and machine learning into existing frameworks for data and intelligence analysis is challenging due to the sheer volume and complexity of the data. The nomination of senior officers in U.S. government agencies in charge of AI strategies and policies is a step in the right direction to ensure risk mitigation, successful use cases and acquisition strategies.

Implement the National Cybersecurity Strategy

The 2024 National Cybersecurity Strategy seeks to secure the digital ecosystem for all Americans and is built around the following five pillars:

1. **Defend Critical Infrastructure:** The goal is to enhance protections for essential systems and networks that underpin American society's everyday functions.
2. **Disrupt and Dismantle Threat Actors:** The country must intensify efforts to identify, prosecute, and dismantle individuals and groups that threaten cybersecurity.
3. **Shape Market Forces to Drive Security and Resilience:** The government must modify economic incentives and regulations to promote security by design in technology development and deployment.
4. **Invest in a Resilient Future:** The nation must commit to advancing cybersecurity through continuous research and development to keep pace with evolving threats.
5. **Forge International Partnerships to Pursue Shared Goals:** The U.S. must collaborate with global allies to bolster collective cybersecurity defenses and respond to incidents more effectively.

Continued implementation of the strategy in coordination and partnership with the private sector remains critical.

Addressing Workforce Shortages

Demographic shifts (i.e., an aging population) may lead to as many as 85 million unfilled jobs by 2030. Addressing workforce shortages requires creative approaches to draw in and keep skilled individuals with the required security clearances. Recommendations include offering more adaptable career paths, improving training programs, and providing incentives to encourage professionals to join the intelligence community.

EXAMPLE: FUTURE-READY WORKFORCE INITIATIVE

The National Security Agency (NSA) has actively responded to workforce shortages with its Future-Ready Workforce Initiative. This program introduces a recruitment strategy known as the '3 Rs'—recruit, retain, and return. It aims to attract not only new entry-level employees but also mid-career professionals and "boomerang" employees who have previously worked at the agency. The NSA seeks to keep its workers happy by offering flexible working conditions (remote or hybrid schedules), improving the employee experience and retention.

Updating AI Strategies and Policies

The White House is already working toward updating strategies and policies around AI. President Biden issued a landmark Executive Order designed to ensure the U.S. leads in harnessing and safely managing artificial intelligence. This strategy focuses on enhancing AI safety and security, protecting privacy, promoting equity, and advancing American leadership globally.

Key actions include establishing new safety standards for AI development, mandating disclosure requirements for developers of significant AI systems, and strengthening AI's application in critical infrastructure through rigorous testing and standards. The strategy also emphasizes the development of tools to detect AI-generated content and safeguard Americans from AI-enabled fraud and deception.

Leveraging Data, Data Management Tools, and Advanced Analytics

The intelligence community needs sophisticated data management tools and analytics to handle the massive amounts of information it encounters. Utilizing sophisticated methods such as machine learning can enhance how the community processes, merges, and analyzes extensive datasets, significantly improving its intelligence-gathering and decision-making capabilities.

Additionally, the Intelligence Community Data Strategy for 2023-2025 focuses on enhancing the management and utilization of data as a strategic asset to support the country's national security goals. It seeks to make data more interoperable, discoverable, and ready for AI applications across all intelligence community elements. It also outlines efforts to advance digital and data innovation partnerships and transform the intelligence community workforce to be more data-driven so data can be securely accessed and leveraged at mission speed.

Encouraging Open-Source Intelligence

The rise of open-source information has made intelligence gathering a more widespread and inclusive activity, extending beyond traditional government circles. This has resulted in a broader network of intelligence contributors, not all of whom are part of the government.

The government must find the best ways to tap into this wealth of data and expertise, then blend it effectively into their broader intelligence analyses. The IC OSINT Strategy 2024-2026 is welcome news and will support the coordination of open source acquisition, sharing, and innovation.

Open-Source Intelligence in Action

Before the invasion of Ukraine, open source intelligence (OSINT) researchers were paying attention to social media posts from Russian accounts that showed trains loaded with tanks and armored vehicles. By geolocating these photos and following the train tracks, researchers were able to identify a massive military buildup not just along the Russia-Ukraine border but also near Belarusian and Moldavian borders. This use of publicly available information, combined with the collective effort of the OSINT community, helped in documenting and understanding the scale and scope of the military movements in real time, providing valuable insights into the unfolding on the ground

Streamlining Procurement Systems

The swift evolution of technology highlights the necessity for a more agile government procurement system and the refinement of the Federal Risk and Authorization Management Program (FedRAMP). FedRAMP standardizes security assessments for cloud products and services used within U.S. government agencies but has faced criticism for its slow, costly, and inconsistent processes across agencies. These challenges hinder agency access to critical technologies and pose significant barriers to entry for smaller companies that lack the resources to navigate the system.

RECOMMENDATIONS

To address these issues and streamline the FedRAMP process, several recommendations have been proposed:

- Re-use of Existing Authorizations: Agencies should be mandated to re-utilize existing authorizations for cloud services to reduce redundancy and expedite the adoption of secure and necessary technologies.
- Designated Agency Leads: Assigning specific leads within each federal agency could ensure more coordinated and efficient interactions with FedRAMP, smoothing out the authorization process.
- Innovative Pilot Programs: Initiating pilot programs to explore new methods for reviewing and authorizing cloud services could lead to more efficient practices and potentially overhaul FedRAMP's operational framework.
- Increased Resources: Providing additional resources to FedRAMP could enable faster review and evaluation of cloud services, making the process more agile and cost-effective.

Additionally, the Department of Defense (DoD) must stay at the forefront of innovation, particularly by supporting rapid prototyping through initiatives at the DIU and offices that report to the Under Secretary of Defense for Research and Engineering. These groups use Other Transaction Authorities (OTAs) to speed up the acquisition of state-of-the-art technologies more efficiently than traditional procurement methods.

These strategic investments and the use of OTAs showcase the DoD's commitment to harnessing commercial technologies for defense purposes, ensuring the U.S. stays ahead in technological capabilities. This proactive strategy not only makes the procurement process smoother but also opens doors for non-traditional defense contractors and tech startups to play a role in national security and defense projects. The IC should also leverage OTAs and other agile acquisition methodologies to bring in new capabilities and tools in support of mission at a quicker pace.

Two Six Technologies: Fortifying America's Defenses

Working with an experienced partner is key to helping the intelligence community and other national security stakeholders adopt the technology they need to keep our country safe in the digital age. Two Six Technologies creates cutting-edge solutions vital for America's conflict deterrence, safety enhancement, and trust building.

Collaborating with our national security partners, Homeland Security, and global allies, we deliver cutting-edge cyber defense and operational technologies. Our innovations support cybersecurity and information operations, including the detection and analysis of misinformation, disinformation, and influence campaigns. Additionally, our solutions enhance systems interoperability and support rapid research and prototyping across various domains.

PRODUCTS INCLUDE:

- **IKE** An orchestration, automation, and analysis platform for all-domain command and control and ML-enabled decision support.
- **M3** Combines AI-powered technology and world class expertise to decode and assess foreign governments' efforts to manipulate narratives in the Information Environment.
- **PULSE** An AI-powered information advantage platform that collects data, generates insights and enables direct engagement with hard-to-reach audiences around the world..
- **SIGMA** A sensor data aggregation platform to detect threats from CBRNE and other critical sensors enabling real-time situational awareness and effective operational response.
- **TRUSTED KEEP** A zero-trust engine purpose-built to protect highly sensitive data at scale—at rest, in transit, and in use—in accordance with U.S. executive requirements.
- **circuitRE** A reverse engineering tool that helps in understanding and analyzing microelectronic components, aiding in vulnerability assessment and the development of defensive measures against hardware-based threats.

Learn more about how Two Six Technologies supports national security initiatives at [TWOSIXTECH.COM.](TWOSIXTECH.COM)

twosix TECHNOLOGIES