https://doi.org/10.59862/k7m2x9q4r8/01

Chapter I

Balancing Security And Innovation: A Policy Perspective

NIKLAS SWANSTRÖM
Director at the Institute for Security & Development Policy (ISDP)*
ORCID 0000-0003-2326-4634

FILIP BORGES MÅNSSON
MA Student at the Military History Department of the Swedish Defence University
ORCID 0009-0006-0681-279X

Abstract: This paper examines the evolving tension between fostering open, collaborative innovation and safeguarding national, economic, and induvial security in an era marked by rapid technological change and increasingly assertive authoritarian actors. Through an analysis of emerging technologies, including Artificial Intelligence (AI), quantum computing, biotechnology, and the internet of things (IOT's), we highlight how innovation simultaneously strengthens and undermine security. The paper concludes by offering a series of policy recommendations aimed at enabling governments to protect critical assets, maintain strategic autonomy, and preserve the benefits of international research cooperation without compromising security.

Keywords: Security, innovation, quantum computing, IP, biotechnology, AI, cybersecurity, dual-use technology, OSINT, cooperation

* Fellow at the Foreign Policy Institute of the Paul H. Nitze School of Advanced International Studies (SAIS) Senior Associate Research Fellow at the Italian Institute for International Political Studies (ISPI)

Policy

In the 21st century, the dual imperatives of maintaining security and fostering innovation have become increasingly intertwined and complex. As nations strive to protect their citizens, infrastructure, and economic interests, they must simultaneously cultivate an environment encouraging technological advancement and creative problem-solving. Much of this innovation is based on international cooperation, exchanges of researchers ranging from basic research at universities to high tech research institutions. These exchanges are crucial for innovation but increases the risk of brain drain, Intellectual Property (IP) theft, and enhances the abilities of hostile states. This delicate balance between security and innovation is crucial for national prosperity, competitiveness, and long-term stability.

Authoritarian states have increasingly been associated with hostile actions in research and innovation, ranging from IP theft to hostile takeovers of companies. China has been noted as one of the most active and successful states when it comes to threats to the European science and innovation security, but simultaneously crucial for some of Europe's innovation and supply chain in sectors such as green technology and rare earth minerals.[1]

The rapid pace of technological change has created new vulnerabilities and security challenges, from sophisticated cyber threats to the potential misuse of artificial intelligence and biotechnology. Concurrently, these same technological advancements offer unprecedented opportunities for economic growth, improved quality of life, and solutions to global challenges such as climate change and healthcare crises. It has famously been noted that expanded supply chain dependency has been the core of our economic development, but also our increased insecurity and dependency on authoritarian states such as Russia and China. Similarly in research and innovation, there would not have been such a rapid progress without the free exchanges of research and innovation, but at the same time it has been misused by authoritarian states that have stolen individual researchers' products, but more importantly put European nations at risk and in a dependency position toward such authoritarian states.

[1] Niklas Swanstrom, Fredrik Erixon and Mrittika Guha Sarkar, *The U.S. and EU, and the Emerging Supply Chain Network: Politics, Prospects & Allies,* (Armin Lear Press 2024).

This paper aims to provide a comprehensive framework for understanding and addressing the tension between security and innovation, and to examine how we best can secure both innovation and security. By examining current trends, and drawing insights from various sectors, we seek to offer practical policy recommendations that can help strike an optimal balance.

The following sections will delve into the intricate relationship between security and innovation, explore the current global landscape, and propose strategies for policymakers to navigate this complex terrain. Our goal is to contribute to the development of policies that not only protect against current and future threats but also unleash the full potential of human ingenuity and technological progress.

The Security-Innovation Nexus

In today's interconnected world, the concept of security has expanded far beyond traditional notions of military defense. It now encompasses a wide range of domains, including, but not limited to:

a. Cybersecurity, which involves protecting digital infrastructure, data, and online systems from attacks and unauthorized access.
b. Economic security, focusing on safeguarding national economic interests, intellectual property, and critical industries.
c. National security, aiming at defending against both conventional and unconventional threats to sovereignty and national interests.
d. Individual security, which focuses on protecting individuals from IP theft, economic sustainability, and social security.
e. Environmental security, addressing climate change and other environmental challenges that pose risks to stability and well-being.
f. Health security, which aims at protecting populations from pandemics and other health crises.

This multifaceted nature of security requires a holistic approach that considers the interplay between various domains and the role of innovation in both creating and mitigating risks. The challenge many times is that there is separate legislation and understanding between the fields as well as a diversified political spectrum with opposing political views, something that might

not be the case in regard to malign actors. Notably there are very different perspectives on what is important in each state. Europe would, as one example, focus on individual security, while China would disregard that aspect and focus on national security. This is something that will increase the challenges in terms of solutions to many of the problems, such as regulations of artificial intelligence (AI) and quantum computing. Many of the different focuses could also be perceived to be in conflict with each other, such as environmental and economic security.

The Role of Innovation in Economic Growth and National Competitiveness

Innovation stands as a fundamental pillar of modern economic development and national competitive advantage. In today's rapidly evolving global landscape, a nation's capacity to innovate has become increasingly crucial in determining its economic prosperity, international standing, and security, and history has shown that innovation is best done without interference of government regulations.[2] Innovation drives economic growth, enhances productivity, strengthens national competitiveness, and enables states to address critical societal challenges; failure to innovate leads to economic stagnation or decline.

Innovation has always served as a powerful engine of economic growth by creating new industries, products, and services while transforming existing ones. When organizations and individuals develop novel solutions to market needs, they generate new economic opportunities that ripple throughout the economy. This process creates jobs, stimulates investment, and generates wealth across multiple sectors. Innovation-driven growth is particularly valuable because it often creates high-skilled, well-paying positions that contribute to the development of a knowledge-based economy. That said, it is dangerous to focus only on innovation and outsource production, as that also creates a dependency that could be challenging, especially as innovation

[2] Philippe Aghion, Antonin Bergeaud and John Van Reenen, "The Impact of Regulation on Innovation," *Cato Institute*, April 19, 2023, https://www.cato.org/research-briefs-economic-policy/impact-regulation-innovation.

and research can be obtained by illegal or legal means, as theft or hostile takeover of companies.[3]

The economic impact of innovation extends far beyond direct effects. When companies introduce innovative products or processes, they often create positive externalities that benefit the broader economy. These spillover effects can include knowledge transfer between industries, the development of supporting sectors, and the creation of new market opportunities for other businesses. Furthermore, innovative activities tend to cluster geographically, leading to the development of innovation hubs that attract talent, investment, and additional innovative enterprises.[4]

Additionally, innovation plays a crucial role in driving productivity growth, which is essential for long-term economic prosperity. Through technological advancements and process improvements, organizations can produce more output with the same or fewer inputs, leading to increased efficiency and reduced costs. This productivity enhancement occurs through various channels, including automation of routine tasks, optimization of production processes, and implementation of more effective management practices.

The impact of innovation on productivity is particularly evident in the digital age. Digital technologies and their applications have revolutionized how businesses operate, enabling unprecedented levels of efficiency and creating new possibilities for value creation. Cloud computing, artificial intelligence, and the Internet of Things have become powerful tools for productivity enhancement, allowing organizations to streamline operations, make data-driven decisions, and better serve their customers.

In the international arena, innovation has become a key determinant of national competitiveness. Countries that foster strong innovation ecosystems typically enjoy advantages in international trade, attract more foreign investment, and maintain higher standards of living for their citizens. A nation's innovative capacity depends on its ability to develop and maintain effective

[3] Swanstrom, Fredrik and Guha Sarkar, *The U.S. and EU, and the Emerging Supply Chain Network: Politics, Prospects & Allies*.

[4] McKinsey & Company, "A Playbook for Innovation Hubs and Ecosystems," *Global Institute for Innovation and Development*, February 28, 2023, https://giid.org/app/uploads/2024/03/A-playbook-for-innovation-hubs-and-ecosystems-McKinsey.pdf.

national innovation systems—complex networks of institutions, policies, and practices that support the creation and diffusion of new technologies and knowledge.

Successful national innovation systems typically feature strong collaboration between academia, industry, and government. Universities and research institutions generate new knowledge and train skilled workers, while businesses transform innovations into marketable products and services. Governments play a crucial role by funding basic research, establishing supportive regulatory frameworks, and ensuring adequate protection of intellectual property rights.

The COVID-19 pandemic demonstrated the critical importance of innovation in addressing global challenges. The rapid development of vaccines, adaptation of business models, and creation of new digital solutions showcased how innovation can help societies respond to unprecedented challenges. This experience highlighted the value of maintaining robust innovation capabilities as a form of societal resilience, and it also highlighted the dangers of being dependent on foreign innovations.

Looking forward, the pace of innovation is likely to accelerate, driven by advances in fields such as AI, biotechnology, and quantum computing. Nations that wish to maintain or enhance their competitive positions must continually adapt their innovation strategies to address emerging challenges and opportunities. This includes ensuring that innovation efforts are sustainable, inclusive, and aligned with societal values.

Innovation remains essential for economic growth and national competitiveness in an increasingly complex global environment. Success in the innovation economy requires a sustained commitment to building and maintaining effective innovation ecosystems, fostering collaboration across sectors, and ensuring that innovation efforts address economic and societal needs. As the world faces unprecedented challenges and opportunities, the ability to innovate effectively will become even more crucial for national success and societal well-being.

The Tension Between Security and Innovation

The relationship between security and innovation presents one of the most complex challenges in modern policymaking. While both elements are fundamental to national prosperity and development, they often appear to work at cross-purposes, creating what many observers describe as an inherent tension.[5] This contribution explores the multifaceted nature of this tension, its implications for various stakeholders, and potential approaches to managing these competing demands.

The apparent conflict between security and innovation stems from their fundamentally different orientations toward risk and change. Security, by its nature, seeks to protect, preserve, and maintain stability. It emphasizes controlled environments, predictable outcomes, and risk mitigation. Innovation, conversely, thrives on disruption, embraces uncertainty, and often requires challenging established norms and practices, and not to mention cross-border cooperation in complex environments.

This divergence manifests in practical tensions across various domains. In organizational settings, security protocols may restrict access to resources or information that could fuel innovative thinking. In technological development, security requirements might constrain the exploration of novel solutions or limit the ability to rapidly iterate and test new ideas. At a national level, security considerations might influence research funding priorities or restrict international collaboration opportunities that could drive innovation.

The tension between security and innovation is perhaps most evident in approaches to risk management. Security frameworks typically adopt a preventative stance, seeking to identify and mitigate potential threats before they materialize. This approach often leads to the implementation of strict controls, detailed documentation requirements, and multiple layers of oversight.[6] While these measures serve important protective functions, they can create significant barriers to innovation, which often requires rapid

[5] Jack Corrigan, Melissa Flagg and Dewey Murdick, "The Policy Playbook," *Center for Security and Emerging Technology* (2023): 8–9, https://doi.org/10.51593/20230018.

[6] Forbes Technology Council, "Benefits And Cautions Of Aligning With Cybersecurity Frameworks," *Forbes*, February 13, 2024, https://www.forbes.com/councils/forbestechcouncil/2024/02/13/benefits-and-cautions-of-aligning-with-cybersecurity-frameworks/.

experimentation, acceptance of failure, and the ability to pivot quickly based on new information or opportunities.

The challenge of balancing these competing approaches to risk becomes particularly acute in sectors such as cybersecurity, biotechnology, and AI, where innovation capabilities directly impact security outcomes. Organizations and policymakers must grapple with questions of how much risk is acceptable, how to evaluate potential benefits against potential threats, and how to create frameworks that protect essential interests without stifling beneficial innovation.

Another critical dimension of the security-innovation tension involves the management of information and knowledge. Innovation typically flourishes in environments characterized by open exchange of ideas, cross-pollination of concepts, and broad collaboration across different domains and organizations. Security considerations, however, often necessitate restrictions on information sharing, implementation of need-to-know protocols, and limitations on external collaboration.

This tension becomes particularly pronounced in research and development settings, where breakthrough innovations often emerge from unexpected connections and cross-disciplinary and cross-border insights. Security requirements that compartmentalize information or limit external engagement can inadvertently create silos that impede creative problem-solving and innovation. The challenge extends to international collaboration, where security concerns about technology transfer or intellectual property protection must be balanced against the benefits of global innovation networks. This is not least a concern realizing that IP theft and espionage in academic and commercial settings.

The allocation of limited resources presents another significant manifestation of the security-innovation tension. Organizations and nations must make difficult decisions about how to distribute financial, human, and technological resources between security initiatives and innovation programs. These decisions are complicated by differences in how security and innovation investments are evaluated and measured.

Security investments often focus on preventing negative outcomes and establishing defenses against intrusion, making their value difficult to quantify

directly. Innovation investments, while potentially offering higher returns, come with greater uncertainty and longer time horizons for realizing benefits.[7] This asymmetry in evaluation metrics can lead to bias toward security investments, particularly in risk-averse organizations or during periods of heightened security concerns.

The tension between security and innovation, while real, need not be viewed as an insurmountable obstacle. Success in the modern environment requires developing sophisticated approaches that can accommodate both imperatives. This demands careful attention to institutional design, policy frameworks, and organizational culture, as well as recognition that security and innovation can, in many cases, be mutually reinforcing rather than exclusively competing priorities.

Moving forward, the key challenge for leaders and policymakers will be to develop nuanced approaches that can protect essential security interests while maintaining the flexibility and openness necessary for innovation to flourish. This requires ongoing dialogue between security and innovation stakeholders, creative approaches to risk management, and commitment to finding balanced solutions that serve both immediate security needs and longer-term innovation goals.

Innovation Trends and Their Security Implications

The rapid pace of technological innovation is fundamentally reshaping our world, bringing both unprecedented opportunities and complex security challenges, at a rapidly increasing phase. As emerging technologies transform industries and societies, they create new vulnerabilities and threats while simultaneously offering novel solutions to security challenges, even if the creation of a secure environment is too often reactive rather than proactive. This segment explores the intricate relationship between major innovation trends and their security implications, examining how these developments are reshaping our approach to security in the modern age.

[7] ISACA, "Quantifying information risk and security," *ISACA Journal*, July 1, 2013, https://www.isaca.org/resources/isaca-journal/past-issues/2013/quantifying-information-risk-and-security.

Artificial Intelligence and Machine Learning: Reshaping Security Paradigms

The emergence of AI and machine learning represents perhaps the most transformative technological shift of our era, fundamentally altering the security landscape. In the defensive realm, AI systems are revolutionizing threat detection and response capabilities. Advanced machine learning algorithms can analyze vast amounts of data to identify patterns indicative of security threats, enabling proactive rather than reactive security measures. These systems are particularly powerful in cybersecurity, where they can detect anomalies and potential attacks in real-time, often identifying threats that would be impossible for human analysts to spot.

However, the same capabilities that make AI powerful for defense also create significant security concerns. Adversaries can leverage AI to develop more sophisticated attack methods, from advanced malware that adapts to defensive measures to deep fakes that can deceive even careful observers. The potential for autonomous weapons systems raises profound ethical and security questions about the role of human judgment in military decisions and the possibility of uncontrolled escalation in conflicts. Moreover, AI still possesses the inherent flaw that it can still be biased and prone to make mistakes, notably in terms of machine learning. Slight alterations can have profound consequences, potentially resulting in the AI being used in an unauthorized manner and as a tool for theft, misuse, and manipulation of data by adversaries.[8]

The Internet of Things: The Challenge of Securing a Connected World

The proliferation of Internet of Things (IoT) devices is creating a more connected and intelligent world but also introducing new security vulnerabilities at an unprecedented scale. Smart city technologies offer tremendous potential for improving public safety and emergency response through better monitoring and coordination of urban systems. Connected sensors and devices

[8] OECD, "Assessing potential future artificial intelligence risks, benefits and policy imperatives," *OECD Artificial Intelligence Papers*, No. 27 (2024): 19–25, https://doi.org/10.1787/3f4e3dfb-en.

can provide early warning of natural disasters, monitor critical infrastructure, and optimize emergency services deployment.

Yet the massive expansion of connected devices creates an equally massive attack surface for cyber threats. Many IoT devices lack robust security features, making them vulnerable to compromise. The interconnected nature of IoT systems means that a breach in one component can potentially compromise entire networks. Privacy concerns are particularly acute, as IoT devices collect vast amounts of personal and behavioral data that could be exploited by malicious actors.[9]

5G and Beyond: The Infrastructure of Future Security

The deployment of 5G, and 6G, networks and the development of future telecommunications technologies promise to transform security capabilities through enhanced communication and data processing capabilities. These networks will enable new applications in emergency response, surveillance, and security monitoring, with the potential for real-time coordination of complex security operations. The increased bandwidth and reduced latency of 5G networks could revolutionize everything from drone operations to remote medical procedures.

However, the fundamental role of these networks in critical infrastructure creates significant security concerns. The complexity of 5G networks introduces new vulnerabilities that could be exploited by sophisticated attackers.[10] Concerns about foreign technology providers and the potential for built-in backdoors or vulnerabilities have made 5G deployment a matter of national security debate in many countries. The need to secure these networks while maintaining their performance benefits presents a major challenge for security professionals.

---

[9] CISA, NSA, FBI, NCSC-UK, ACSC, CCCS and NCSC-NZ, "Cybersecurity Best Practices for Smart Cities", April 19, 2023, https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf.

[10] Tom Wheeler and David Simpson, "The digital future requires making 5G secure," *Brookings Institution*, December 12, 2022, https://www.brookings.edu/articles/the-digital-future-requires-making-5g-secure/.

Looking Beyond 5G, the anticipated deployment of 6G networks will continue to redefine connectivity standards and have transformative implications for society and security alike. As it will most likely integrate even deeper with AI and IoT, the need to ensure and address the current challenges we face with 5G is essential as the risks of privacy intrusions, data exploitation, and network manipulation by malicious actors will continue to pose significant challenges and may grow exponentially, as new network iterations such as 6G is likely have its own intricate flaws once developed and deployed.

Quantum Computing: The Next Frontier of Cryptographic Security

Quantum computing represents both a revolutionary advance in computational capabilities and a fundamental challenge to current security paradigms. The potential of quantum computers to solve complex problems could transform fields ranging from drug discovery to climate modeling. In the security domain, quantum computing offers the possibility of unbreakable encryption methods and advanced threat detection capabilities, but reversely also unbreakable threats to individual and government security.

However, the same computational power that makes quantum computers revolutionary also threatens to render current encryption methods obsolete. The ability of quantum computers to factor large numbers quickly could break many current cryptographic systems, potentially exposing sensitive data and communications. This has sparked a race to develop quantum-resistant cryptography before practical quantum computers become a reality.

Moreover, the implications of quantum computing extend beyond cryptography and pose challenges to broader aspects of cybersecurity infrastructure. Notably, blockchain technologies, widely considered secure due to their reliance on asymmetric cryptography, could potentially be undermined by quantum decryption capabilities.[11] The global race to harness quantum computing is also intensifying geopolitical tensions, as nations seek to develop quantum technologies for both defensive and offensive purposes. In this con-

[11] Deloitte, "Quantum computers and the Bitcoin blockchain," *Deloitte Netherlands: Risk Advisory Perspectives*, 2023, https://www.deloitte.com/nl/en/services/risk-advisory/perspectives/quantum-computers-and-the-bitcoin-blockchain.html.

text, the emergence of "quantum supremacy"—the point at which quantum computers surpass classical computers in solving specific tasks—could reshape power dynamics in both commercial and military domains.

Biotechnology and Synthetic Biology: The Frontier of Biosecurity

Advances in biotechnology and synthetic biology are revolutionizing our ability to understand and manipulate biological systems. These capabilities have demonstrated their value during the COVID-19 pandemic, enabling rapid vaccine development and new approaches to disease detection and treatment. The potential for personalized medicine and advanced diagnostic tools offers tremendous promise for public health and security.

Yet these same advances raise serious biosecurity concerns, notably the rise of global pandemics has made governments and individuals realize the potential vulnerability. The ability to engineer biological systems are prone to risk of dual-use and could be misused to create enhanced pathogens or biological weapons.[12] The democratization of biotechnology tools and techniques makes it increasingly difficult to control who has access to these capabilities. Ensuring the security of biological research while maintaining its benefits for human health and development represents a critical challenge. Simultaneously, the development of biosecurity could be an asset internationally that should be seen as a common resource, if not the dangers of being misused was so high.

Successes and Failures in Balancing Security and Innovation: DARPA and OSINT in Ukraine

The relationship between security and innovation is complex and multifaceted, often requiring careful balance between competing priorities. Two compelling case studies—DARPA's institutional approach to fostering innovation and the role of OSINT in the Ukraine conflict – provide valuable insights into how organizations and actors navigate these challenges in practice[13]. These

[12] Benjamin D. Trump, "Biosecurity for Synthetic Biology and Emerging Biotechnologies: Critical Challenges for Governance," September 8, 2021, https://www.ncbi.nlm.nih.gov/books/NBK584259/.

[13] Swanstrom. Erixon and Guha Sarkar, T*he U.S. and EU, and the Emerging Supply Chain Network: Politics, Prospects & Allies.*

cases illustrate different aspects of the security-innovation relationship and offer lessons for future policy and practice.

DARPA: Institutionalizing Innovation in National Security

The Defense Advanced Research Projects Agency (DARPA) emerged from the Cold War need to prevent strategic technological surprise, following the Soviet Union's launch of Sputnik. Since its inception in 1958, DARPA has evolved into a unique institution that successfully bridges the gap between security requirements and innovative research.[14] Its organizational structure and operational approach offer valuable insights into how to foster innovation while serving national security objectives.

DARPA's success stems from several key organizational characteristics that enable it to balance security and innovation effectively. The agency maintains a relatively small, flat organization with rotating program managers who serve limited terms. This approach brings fresh perspectives and prevents institutional stagnation. DARPA's program managers have significant autonomy in project selection and management, allowing them to pursue promising but risky ideas that might be overlooked in more traditional research organizations.

The agency's funding model emphasizes high-risk, high-reward projects that might not find support through conventional channels. By accepting a higher failure rate than traditional research organizations, DARPA creates space for truly transformative innovations. This approach has led to breakthrough developments in areas ranging from the internet to stealth technology, demonstrating how security objectives can drive broader technological innovation.

One of DARPA's most significant contributions has been its ability to develop technologies with both military and civilian applications. The internet, GPS, and voice recognition software all emerged from DARPA-funded research. This dual-use approach helps justify investment in high-risk research while ensuring that innovations benefit both national security and econo-

[14] "About DARPA," DARPA, accessed November 19, 2024, https://www.darpa.mil/about-us/about-darpa.

mic development. It also creates pathways for technology transfer between defense and civilian sectors, maximizing the impact of research investments.

DARPA has developed sophisticated approaches to managing security concerns while maintaining the openness necessary for innovation. The agency carefully segments research projects, maintaining appropriate security controls while allowing sufficient information sharing to drive innovation. This balanced approach has enabled DARPA to work effectively with both classified defense programs and open academic research. This noted, the DARPA model should primarily be implemented among like-minded states, or even among allies in some cases.

OSINT in the Ukraine Conflict: Innovation in Real-Time Intelligence

The conflict in Ukraine has demonstrated the revolutionary potential of open-source intelligence (OSINT) in modern warfare and international security.[15] Social media platforms, commercial satellite imagery, and other publicly available data sources have created unprecedented transparency in conflict zones, fundamentally changing how information is gathered, analyzed, and disseminated.

The Ukraine conflict has spawned numerous innovations in OSINT collection and analysis. Civilian analysts and researchers have developed new techniques for verifying and correlating information from multiple sources, creating detailed pictures of military movements and operations. Social media monitoring tools, geolocation techniques, and collaborative analysis platforms have evolved rapidly in response to the conflict's demands.[16]

The proliferation of OSINT capabilities has challenged traditional approaches to operational security. Military operations that once could be conducted with relative secrecy are now visible to anyone with internet access

[15] Robin Kemp, "OSINT's influence on the Russian air campaign in Ukraine and the implications for future western deployments," *Atlantic Council*, August 30, 2022, https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/osints-influence-on-the-russian-air-campaign-in-ukraine-and-the-implications-for-future-western-deployments/.

[16] Owen Vandersmith, "How Open-Source Intelligence Is Changing Warfare," *US Naval Institute*, March 2023, https://www.usni.org/magazines/proceedings/2023/march/how-open-source-intelligence-changing-warfare.

and basic analytical skills. This transparency has forced military planners to adapt their approaches to operational security while also creating new opportunities for strategic communication and information operations.

OSINT has democratized access to intelligence information, allowing non-state actors, including journalists, researchers, and civilian analysts, to conduct sophisticated intelligence analysis.[17] This development has profound implications for international security, creating new channels for verification of claims and counter-propaganda, while also raising concerns about the potential misuse of sensitive information.

The widespread availability of OSINT capabilities has created new security challenges. Military forces must now operate under constant surveillance from civilian observers, requiring new approaches to operational security. The risk of disinformation and manipulation of open-source information has also emerged as a significant concern, requiring careful verification and analysis procedures.

Lessons Learned

Both cases demonstrate the importance of institutional frameworks in managing the security-innovation relationship. DARPA's structured approach to fostering innovation while maintaining security controls offers lessons for other organizations seeking to balance these competing demands. The OSINT community's development of collaborative verification and analysis methods shows how informal institutions can emerge to address new security challenges.

Both DARPA and the OSINT community in Ukraine demonstrate the importance of adaptability in responding to technological change. DARPA's rotating leadership and focus on emerging technologies help it stay ahead of technological trends, while the OSINT community's rapid development of new analytical techniques shows how innovation can occur in response to immediate operational needs.

---

[17] H.I. Sutton, "Reflecting on One Year of War: The Power of Open-Source Intelligence," *Center for Maritime Strategy*, February 6, 2023, https://centerformaritimestrategy.org/publications/reflecting-on-one-year-of-war-the-power-of-open-source-intelligence/.

Both cases also highlight the challenges and opportunities in managing information flows in security contexts. DARPA's segmented approach to research security and the OSINT community's development of verification procedures offer different models for balancing openness with security requirements.

These case studies demonstrate that the relationship between security and innovation is not simply antagonistic but can be managed productively through appropriate institutional frameworks and operational practices. DARPA's success in fostering breakthrough innovations while serving national security needs shows how organizational design can help balance competing priorities. The evolution of OSINT in the Ukraine conflict illustrates how technological innovation can transform security practices while creating new challenges that require innovative solutions.

The lessons from these cases suggest that successful management of the security-innovation relationship requires:

- Flexible institutional frameworks that can adapt to changing circumstances.
- Clear processes for managing information and security requirements.
- Support for experimentation and acceptance of calculated risks.
- Recognition of the potential for dual-use applications of new technologies.
- Continuous adaptation to evolving technological capabilities and security challenges.

Key Considerations for Policymakers

To ensure an effective balance between security and innovation, policymakers should consider:

1. Adaptive and Risk-Based Regulatory Frameworks

Policymakers should implement flexible and adaptive regulatory approaches that can evolve alongside rapid technological advancements. A risk-based framework is essential, prioritizing security measures according to the potential risks associated with specific technologies or sectors. This helps ensure that regulations remain relevant and effective without stifling innovation.

2. Regulatory Sandboxes and Dual-Use Technology Safeguards
Regulatory sandboxes allow for the testing of innovative technologies in a controlled environment under regulatory supervision. In parallel, safeguarding policies for dual-use technologies (those with both civilian and military applications) are vital. These policies should ensure that while the benefits for civilian use are promoted, the risks of misuse for military or harmful purposes are minimized.

3. Strengthening Intellectual Property Laws and Cybersecurity
Strengthening intellectual property (IP) laws and enforcement mechanisms is crucial for protecting research from theft or exploitation by hostile foreign entities. This includes fostering closer collaboration between the government and private sector to secure technological innovations, especially in high-risk sectors such as AI, cybersecurity, and biotechnology.

4. Investment in Quantum Computing and Digital Security Research
Governments should prioritize investment in quantum computing research, particularly in the development of quantum-resistant cryptography. These efforts will fortify current and future digital infrastructure, helping safeguard critical systems from potential threats posed by quantum computing capabilities in adversarial hands.

5. Education and Workforce Development in High-Risk Sectors
To maintain a competitive edge, policymakers should focus on incentivizing education and workforce development, particularly in high-risk sectors such as AI, biotechnology, and cybersecurity. Encouraging both public and private sector investment in skills training and education ensures a robust workforce ready to meet the challenges posed by rapidly evolving technologies.

Bibliography

Aghion, Philippe, Antonin Bergeaud and John Van Reenen. "The Impact of Regulation on Innovation." *Cato Institute*, April 19, 2023. https://www.cato.org/research-briefs-economic-policy/impact-regulation-innovation.

CISA, NSA, FBI, NCSC-UK, ACSC, CCCS and NCSC-NZ. "Cybersecurity Best Practices for Smart Cities." April 19, 2023. https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf.

Corrigan, Jack, Melissa Flagg and Dewey Murdick. "The Policy Playbook." *Center for Security and Emerging Technology* (2023): 8–9. https://doi.org/10.51593/20230018.

"About DARPA." DARPA accessed November 19, 2024, https://www.darpa.mil/about-us/about-darpa.

Deloitte. "Quantum computers and the Bitcoin blockchain." *Deloitte Netherlands: Risk Advisory Perspectives*, 2023. https://www.deloitte.com/nl/en/services/risk-advisory/perspectives/quantum-computers-and-the-bitcoin-blockchain.html.

Forbes Technology Council. "Benefits And Cautions Of Aligning With Cybersecurity Frameworks." *Forbes*, February 13, 2024. https://www.forbes.com/councils/forbestechcouncil/2024/02/13/benefits-and-cautions-of-aligning-with-cybersecurity-frameworks/.

ISACA. "Quantifying information risk and security." *ISACA Journal*, July 1, 2013. https://www.isaca.org/resources/isaca-journal/past-issues/2013/quantifying-information-risk-and-security.

Kemp, Robin. "OSINT's influence on the Russian air campaign in Ukraine and the implications for future western deployments." *Atlantic Council*, August 30, 2022. https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/osints-influence-on-the-russian-air-campaign-in-ukraine-and-the-implications-for-future-western-deployments/.

McKinsey & Company. "A Playbook for Innovation Hubs and Ecosystems." *Global Institute for Innovation and Development*, February 28, 2023. https://giid.org/app/uploads/2024/03/A-playbook-for-innovation-hubs-and-ecosystems-McKinsey.pdf.

Swanstrom, Niklas, Fredrik Erixon and Mrittika Guha Sarkar. *The U.S. and EU, and the Emerging Supply Chain Network: Politics, Prospects & Allies*, Armin Lear Press, 2024.

Sutton, H. I. "Reflecting on One Year of War: The Power of Open-Source Intelligence." *Center for Maritime Strategy*, February 6, 2023. https://centerformaritimestrategy.org/publications/reflecting-on-one-year-of-war-the-power-of-open-source-intelligence/.

Trump, Benjamin, D. "Biosecurity for Synthetic Biology and Emerging Biotechnologies: Critical Challenges for Governance." September 8, 2021. https://www.ncbi.nlm.nih.gov/books/NBK584259/.

OECD. "Assessing potential future artificial intelligence risks, benefits and policy imperatives." *OECD Artificial Intelligence Papers*, no. 27 (2024): 19–25. https://doi.org/10.1787/3f4e3dfb-en.

Vandersmith, Owen. "How Open-Source Intelligence Is Changing Warfare." *US Naval Institute*, March 2023. https://www.usni.org/magazines/proceedings/2023/march/how-open-source-intelligence-changing-warfare.

Wheeler, Tom and David Simpson. "The digital future requires making 5G secure." *Brookings Institution*, December 12, 2022. https://www.brookings.edu/articles/the-digital-future-requires-making-5g-secure/.