How innovation impacts global security

by Gazmend Huskaj

Resumé

Artikeln behandlar hur teknologisk innovation påverkar den globala säkerheten, och betonar att framsteg inom områden som informations- och kommunikationsteknik och sammankopplade informationssystem, cyberförmågor och artificiell intelligens (AI) har dubbla användningsområden. Först definieras innovation och global säkerhet. Därefter granskas två fall av cyberspionage, som visar hur hotaktörer exploaterar framsteg inom teknologiska innovationer för att främja sina strategiska mål. Dessa fall understryker de sårbarheter och strategiska förändringar som teknologiska innovationer medför, särskilt i samband med ekonomisk stabilitet och geopolitisk maktbalans. Dessutom behandlas den snabba utvecklingen av AI och dess implikationer för krigföring och global säkerhet. Resultaten visar att det krävs en balanserad strategi för att omfamna teknologiska framsteg för internationell dialog och utnyttjandet av fördelarna med innovation samtidigt som riskerna för den globala säkerheten minskas.

TECHNOLOGICAL ADVANCEMENTS AND innovation are impacting global security. Innovation is a process of inventing new technologies or methodologies and a representation of a broader spectrum of creative thinking and application that leads to transformative changes across various domains.[1] Here, innovation consists of invention and creativity. Invention is the creation of something new (such as a new algorithm, program or software development technique)[2]. Creativity is a state of mind that fosters innovative thinking. Therefore, innovation is the combination of creative acts and inventions that are widely used, leading to substantial kinds of change and the successful exploitation of new ideas. Given the expansive role of innovation, exploring its implications for global security is important. Therefore, how does innovation impact global security?

Global security, just like innovation, can be conceptualized and defined in various ways, contingent upon the level of analysis, the range of perceived threats, and the nature of the actors involved. Here, two definitions are used: the RAND organization and the Cambridge Dictionary. The RAND organization states that global security includes military and diplomatic measures that nations and international organizations such as the United Nations and NATO take to ensure mutual safety and security.[3] The Cambridge Dictionary defines global security as the protection of the world against war and other threats.[4] These definitions are complementary, as they highlight different aspects of global security.

This article shows how some threat actors use/have used innovations in information and communication technologies and interconnected information systems for cyber espionage, affecting economic stability and the geopolitical balance of power. It will also discuss the rapid pace of AI development

and its cascading effects in multiple domains, transcending borders and impacting global security. These examples illustrate the dual-use nature of technological innovations, which can be applied for both civilian and military purposes, thereby creating complex and multidimensional implications for global security.

The article is organized as follows: Section 2 presents the impact of innovation on global security. Section 3 presents cyber espionage cases and analyzes their implications for economic security. Section 4 discusses the rapid development of AI and its implications for warfare. Section 5 concludes the document and provides some recommendations for using the benefits of innovation while reducing the risks.

The impact of innovation on global security

Understanding the impact of innovation on global security requires knowing that this includes the implications of humanity's creative acts and inventions.[5] These implications become significant when they are extended into widespread application, leading to substantial kinds of change. This covers a range of developments, from conventional military hardware like main battle tanks and combat aircraft to more advanced technological innovations such as nuclear weapons, space satellites, and cutting-edge domains like information and communication technologies, the Internet, Artificial Intelligence, and Quantum computing. Therefore, advancements in innovation influence the strategies and measures adopted by various national and international organizations to ensure mutual safety and security.

Cyber security and cyber espionage

Innovations have implications for global security beyond the military domain. An example is cyber security. Cyber security has become increasingly critical. This is a growing concern as more and more activities and services (= software) depend on information and communication technologies and internetworked information systems. Additionally, political and economic stability are also affected by innovations, as they create new opportunities and challenges for policy, trade, development, and competitiveness. Another crucial aspect is environmental sustainability. Innovations can mitigate or exacerbate the effects of climate change, pollution, and resource depletion, impacting global security.[6]

One of the main characteristics of many modern innovations is that they can be used for both civilian and military purposes (dual use).[7] This is especially evident in cyber security, where technological advancements can be utilized for defensive measures and offensive cyberspace operations, enabling, for example, cyber espionage activities.[8]

The following sections will analyze how some threat actors use/have used innovations in information and communication technologies and internet-worked information systems to conduct cyber espionage. This involves exploring the possible ways these technologies can be used to breach security and the wider implications of such actions for global stability, safety and security.

In 2017, a major UK accounting firm[9] and a British multinational defense company, in collaboration with a national cybersecurity agency in the UK, and support from a specific Swedish agency, reported a new cyber espionage campaign carried out by a threat actor, APT10, based in Asia.

The report applied various analytical methods to attribute the cyber espionage campaign to the Asian threat actor. The attackers targeted companies that specialized in managing IT and services for other businesses.[10] These companies had access to their clients' networks, which made them attractive targets. This made the so-called managed service providers (MSPs) attractive targets for cyber espionage. Once the threat actor gains access, it is believed to be relatively easy to exploit this access and potentially move onto the networks of thousands of other victims.[11]

When examining global security, it becomes clear that the interconnection of various innovations is a key aspect impacting it. For example, the cyber espionage operation mentioned above exploited the innovations in interconnected information systems with malicious intent to support the strategic objectives of the Asian country. Extrapolating from this, AI and quantum computing advancements could similarly have significant implications across various sectors, including the public, private, industry, academia, and defense. Innovations in one field, such as AI breakthroughs, may not only improve cyber offense[12] and defense[13] capabilities but also accelerate developments in autonomous weapons systems.[14] These accelerated advancements could alter the geopolitical balance of power. Similarly, advancements in information and communication technologies have transformed how various actors collect intelligence, but they also create vulnerabilities that can be exploited by state and non-state actors alike.[15] This complex set of interdependencies means that an innovation in one field can have cascading effects across multiple domains.[16]

Another cyber espionage case, albeit earlier in time than the one mentioned above, presents how threat actors exploited the complex set of interdependencies due to innovations, threatening economic stability. A cybersecurity firm, which later became part of a larger cybersecurity corporation, released a report in 2013 revealing a multi-year cyber espionage campaign.[17] APT1 conducted a cyber espionage campaign from an Asian country. The targets were in various countries and industries related to the country's strategic objectives. The report indicated that the targeted sectors included information technology, high-tech electronics, financial services, satellite and telecommunications, energy, public administration, scientific research and consulting, chemicals, and aerospace.[18] Evidence linked this threat actor to a particular military unit of the Asian country's armed forces.[19]

The evidence was so convincing that a major Western country's Department of Justice charged individuals from the Asian country.[20] One of the publicly named victims of APT1 was SolarWorld, a solar energy company.[21]

SolarWorld was a global leader in the solar industry when the attacks were exposed, with an annual turnover of €750 million.[22] Its competitive edge was a combination of intellectual property (IP) and extensive global contracts. However, in May 2017, SolarWorld filed for insolvency.[23]

This leads to the question: How does a firm, a market leader in its industry and owner of cutting-edge IP and global contracts, become insolvent so quickly?

Market saturation from a major Asian country, starting around the time of the APT1 attack 2012, contributed to the company's rapid decline.[24]

As the Department of Justice of a major Western country stated: "The perpetrators stole trade secrets that would have been especially beneficial to Chinese companies at the time they were stolen."[25]

The impact on SolarWorld was significant. The company's Director of Strategic Affairs said at the time: "There were thousands of emails exfiltrated, many with sensitive data that would give all kinds of unfair advantages."[26] These unfair advantages included intellectual property, sensitive pricing information, and even methods for competitors from the Asian country to bypass Western regulations and dominate the market.[27]

Since then, the Asian country has become a leading nation in solar energy, exceeding its 2020 solar targets in August 2017 with a significant output. This was around the same time the country cancelled many coal projects, aligning with the "future energy development" goals of its five-year plan for 2016-2020.[28] The simultaneous announcement of this country's solar energy achievements and the insolvency of the solar panel company in the same month is too coincidental. This illustrates the divergent results of APT1's cyber espionage operations, where one entity emerged as a "winner" and the other as a "looser."

On a global level, the impact of innovation in security is not limited to any single nation but affects continents, shaping international relations in various ways.[29] For example, the COVID-19 pandemic revealed vulnerabilities in the supply of semiconductors[30], leading to discussions in the US[31] and Europe[32] to build their factories. Also, the rapid development of AI in the US has stimulated discussions for similar advancements in Asia and Europe.[33] This could lead to a global race for technological supremacy. The race is not only about technological advancements but could also be about setting international norms and standards for using such technologies.[34] The SolarWind ? World? case presents how technological advancements can be used for strategic gains, affecting not only corporate entities but also national and regional economies and geopolitical balances.

In regions like the Middle East and Africa, where technological adoption may vary,[35] innovations in cyber capabilities and unmanned systems by more technologically advanced nations could pose new challenges to regional security dynamics. Similarly, advancements in information and communication technologies have led to increased use of cyber attacks in the Russia-Ukraine war, where the targets are increasingly non-military.

Moreover, the war has acted as a driver of innovation where supporters of Ukraine could conduct cyber attacks on Russian targets by simply downloading an app. The user did not know that the app was collecting all the information on their smartphone, likely sending it to an intelligence agency in Russia.[36]

Furthermore, on 13th of September 2023, a Reuters journalist quoted the President of the European Commission as saying, "Global markets are now flooded with cheaper electric cars, and their price is kept artificially low by huge state subsidies. Europe is open to competition, not a race to the bottom."[37] This statement highlights the EU's determination to avoid repeating the experience of its solar panel industry, which was decimated by cheaper imports from an Asian country. Why? The industry at risk is Europe's car industry, which is threatened by cheaper electric cars from the Asian country.

According to the European Commission, "exports to countries outside the EU reached a peak of €158 billion in 2022."[38] The exact entity states that "the car industry is of prime importance to the economy of the European Union (EU) and plays a major role in international trade."[39] Therefore, the car industry is not only about the EU's economic security but also about the EU's ability to influence. Decimating the car in-

dustry would likely put the EU at a disadvantage in its influence over negotiations in multiple domains.

Thus, from an economic intelligence perspective, the SolarWorld case is an excellent example of how cyber espionage can impact a market capable of wiping out an entire industry. Similarly, the case of electric vehicles demonstrates how innovation, supported by cyber espionage operations and state subsidies, can likely severely affect the economic security of entities like the European Union.

The Rapid Development of AI and Its Implications for Warfare

Another innovation that impacts global security is Artificial Intelligence (AI).

According to a report from Stanford, co-authored with other organizations, the growth of AI computational power followed Moore's Law until 2012. This principle states that computing power roughly doubles every two years. However, after 2012, AI computing began to double at a fast rate of every 3.4 months.[40]

A significant contribution to this acceleration was the 2017 paper "Attention Is All You Need" by researchers from Google Brain and other entities.[41] This paper introduced the Transformer model, a major shift in how AI systems process language. By relying entirely on attention mechanisms, the Transformer model improved efficiency and effectiveness in handling long-range dependencies in data, setting new benchmarks in natural language processing tasks. This innovation spurred further advancements in AI, leading to more sophisticated models like GPT and BERT, and has broad implications for AI's role in global security.

For example, in 2016, researchers developed an Artificial Intelligence model for combat aircraft. When competing against ALPHA, the human pilot said: "I go home feeling washed out. I'm tired, drained, and mentally exhausted. This may be artificial intelligence, but it represents a real challenge."[42]

According to the researchers, the ALPHA AI, designed for combat aircraft, "can act on sensor data to make or change decisions about combat for up to four aircraft in less than a millisecond, moving aircraft to evade missiles and fire weapons while a human pilot essentially manages the overall air battle at a higher level."[43] In 2020, an unnamed AI defeated a US military fighter pilot in an F-16 dogfight, successfully winning five out of five simulated fights.[44] In February 2023, an unnamed artificial intelligence pilot successfully piloted an F-16 fighter jet for over 17 hours.[45] These cases illustrate a shift from human-piloted combat aircraft to so-called "uncrewed" warfare. This case provides a good example showcasing the rapid pace of AI development training with an AI in a simulator in 2016; 2020, flying in aerospace; and 2023 integrated into a combat aircraft.

The evolution of AI capabilities, shown by the Transformer model and its developments, presents various opportunities and challenges in global security. On one hand, these advancements can lead to more efficient data analysis and intelligence collection, improving national security. On the other hand, the same technology could be used for cyber espionage, autonomous weapons systems, and advanced surveillance, creating ethical and strategic concerns. The dual-use nature of AI technologies means their impact on global security is complex, requiring careful consideration and international dialogue to use their benefits while reducing risks.

Conclusion

Thus, the answer to how innovation impacts global security is multidimensional. Firstly, innovation acts as a double-edged sword; on the one hand, it brings about advanced technologies and solutions that enhance a nation's defense capabilities, improves intelligence collection, and increase the ability to protect against various threats. On the other hand, the same innovations can be exploited for malicious purposes like cyber espionage, creating new vulnerabilities and challenges in maintaining global stability, safety and security. This duality necessitates a balanced approach where nations embrace and foster technological advancements while being aware of and prepared for their potential implications on global security.

Secondly, the AI revolution is evolving at a rapid pace. It is crucial to remember that this exponential development and related innovations have cascading effects in multiple domains, transcending borders and impacting global security. The cases of cyber espionage, such as the SolarWorld case, present how innovations in information and communication technologies and internetworked information systems can be exploited for national strategic purposes. While the company went bankrupt, the attacking nation thrived, decimating an entire EU market in solar panels.

The author is the head of Cyber Security at the Geneva Centre for Security Policy.

Notes

1. Rose, Jeremy: "Digital Innovation", *Scientific Theory in Informatics A1N*, University of Skövde, 2019, *http://websvrnu.his.se/rosl/digital-innovation/digital-innovation.html*, (2023-12-13).
2. Ibid.
3. RAND Corporation: "Global Security", *https://www.rand.org/topics/global-security.html*, (2023-12-13).
4. Cambridge Dictionary: "Global Security", 2023, *https://dictionary.cambridge.org/dictionary/english/global-security*, (2023-12-13).
5. Op. cit., Rose, Jeremy, see note 1.
6. Avelar, Luiz: "How Can Technology Help Combat Climate Change", *World Economic Forum*, 2021-07-12, *https://www.weforum.org/agenda/2021/07/fight-climate-change-with-technology/*, (2023-12-13).
7. Vergun, David: "DOD Modernization Relies on Rapidly Leveraging Commercial Technology", *U.S. Department of Defense*, 2023-01-25, *https://www.defense.gov/News/News-Stories/Article/Article/3277453/dod-modernization-relies-on-rapidly-leveraging-commercial-technology/*, (2023-12-13).
8. Ibid.
9. *Operation Cloud Hopper*, PwC & BAE Systems, April 2017, *https://www.pwc.co.uk/cyber-security/pdf/pwc-uk-operation-cloud-hopper-report-april-2017.pdf*, (2023-12-13).
10. Ibid.
11. Ibid.
12. Al-Hawawreh, Muna; Aljuhani, Ahamed and Jararweh, Yaser: "Chatgpt for cybersecurity: practical applications, challenges, and future directions", *Cluster Computing*, 26, pp. 3421-3436, *https://doi.org/10.1007/s10586-023-04124-5*.
13. Alspach, Kyle: "5 Big Pros And Cons Of ChatGPT For Cybersecurity", *CRN*, 2023-01-27, *https://www.crn.com/news/security/5-big-pros-and-cons-of-chatgpt-for-cybersecurity*, (2023-12-13).
14. Abaimov, Stanislav and Martellini, Maurizio: "Artificial Intelligence in Autonomous Weapon Systems" in Martellini, Maurizio and Trapp, Ralf (eds.): *21st Century Prometheus*, Springer, Cham 2020, https://doi.org/10.1007/978-3-030-28285-1_8, s 141-177.
15. Olson, Stephen: "Trade tensions rise on dual use technologies, protectionism and geopolitics", *Hinrich foundation*, 2019-10-30, *https://www.hinrichfoundation.com/research/article/tech/dual-use-technology-trade-tensions/*, (2023-12-13).
16. Ibid.
17. *APT1: Exposing One of China's Cyber Espionage Units*, Mandiant, *https://www.mandiant.com/resources/reports/apt1-exposing-one-chinas-cyber-espionage-units*, (2023-12-13).
18. Ibid.
19. Ibid.
20. U.S. Department of Justice: "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage", 2014-05-19, *https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor*, (2023-12-13).
21. Ibid.
22. Hyvärinen, Noora: "APT1 – what happened next?", *F-Secure*, 2017-09-29, *https://blog.f-secure.com/apt1-what-happened-next/*, (2023-12-13).
23. Ibid.
24. Ibid.
25. Ibid.
26. Ibid.
27. Ibid.
28. Ibid.
29. Danilin, Ivan, V.: "Emerging Technologies And Their Impact On International Relations And Global Security", *Hoover Institution*, 2018-10-03, *https://www.hoover.org/research/emerging-technologies-and-their-impact-international-relations-and-global-security*, (2023-12-13).
30. King, Ian; Wu, Debby and Pogkas, Demetrios: "How a Chip Shortage Snarled Everything From Phones to Cars", *Bloomberg*, 2021-03-29, *https://www.bloomberg.com/graphics/2021-semiconductors-chips-shortage/*, (2023-12-13).
31. Escande, Philippe: "Intel CEO Pat Gelsinger: US and EU's competitive gap with Asia around 40% on semiconductors", *Le Monde*, 2023-12-07, *https://www.lemonde.fr/en/international/article/2023/12/07/intel-ceo-pat-gelsinger-us-and-eu-s-competitive-gap-with-asia-around-40-on-*

semiconductors_6322449_4.html, (2023-12-13).
32. Eddy, Melissa and Liu, John: "Taiwan's Chip Giant Will Build a Plant in Germany", *The New York Times,* 2023-08-08, *https://www.nytimes.com/2023/08/08/world/europe/tsmc-germany-chips-semiconductors.html*, (2023-12-13).
33. Castro, Daniel and McLaughlin, Michael: "Who Is Winning the AI Race: China, the EU, or the United States? — 2021 Update", *Information Technology & Innovation Foundation*, 2021-01-25, *https://itif.org/publications/2021/01/25/who-winning-ai-race-china-eu-or-united-states-2021-update/*, (2023-12-13).
34. Haddad, Mais: "The Race for AI Governance: Navigating the International Regulatory Landscape of Artificial Intelligence", *JURIST – Professional Commentary*, 2023-03-17, *https://www.jurist.org/commentary/2023/03/mais-haddad-international-regulations-artificial-intelligence/*, (2023-12-13).
35. Iftahy, Abdellah; Isherwood, Tom; Marcati, Chiara and Soni, Karan: "Digital consumers in the Middle East: Rising adoption and opportunity", *McKinsey & Company*, 2023-01-09, *https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-consumers-in-the-middle-east-rising-adoption-and-opportunity*, (2023-12-13).
36. Cluley, Graham: "Anti-Russian denial-of-service app actually infects pro-Ukrainian activists", *Bitdefender*, 2022-07-20, *https://www.bitdefender.co.uk/blog/hotforsecurity/anti-russian-denial-of-service-app-actually-infects-pro-ukrainian-activists/*, (2023-12-13).
37. Blenkinsop, Philip: "EU to investigate 'flood' of Chinese electric cars, weigh tariffs", *Reuters*, 2023-09-13, *https://www.reuters.com/world/europe/eu-launches-anti-subsidy-investigation-into-chinese-electric-vehicles-2023-09-13/*, (2023-12-13).
38. Eurostat: "International trade in cars", *European Commission*, 2023-11-06, *https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=328429*, (2023-12-13).
39. Ibid.
40. Saran, Cliff: "Stanford University finds that AI is outpacing Moore's Law", *ComputerWeekly.com*, 2019-12-12, *https://www.computerweekly.com/news/252475371/Stanford-University-finds-that-AI-is-outpacing-Moores-Law*, (2023-12-13).
41. Vaswani, Ashish et al.: "Attention Is All You Need", 31st Conference on Neural Information Processing Systems (NIPS 2017), Long Beach, CA, USA, *https://proceedings.neurips.cc/paper_files/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aa-Paper.pdf*, (2023-12-13).
42. University of Cincinnati: "New artificial intelligence beats tactical experts in combat simulation", *EurekAlert!*, 2016-07-27, *https://www.eurekalert.org/news-releases/782522*, (2023-12-13).
43. Gallagher, Sean: "AI bests Air Force combat tactics experts in simulated dogfights", *ArsTechnica,* 2016-06-29, *https://arstechnica.com/information-technology/2016/06/ai-bests-air-force-combat-tactics-experts-in-simulated-dogfights/*, (2023-12-13).
44. Martin, Alexander: "AI system beats US military pilot in F-16 dogfight", *Sky News*, 2020-08-22, *https://news.sky.com/story/ai-system-beats-us-military-pilot-in-f-16-dogfight-12053815*, (2023-12-13).
45. Keach, Sean: "AI successfully pilots F-16 fighter jet for over 17 hours as US prepares for 'uncrewed' warfare", *The U.S. Sun,* 2023-02-14, *https://www.the-sun.com/tech/7393463/ai-jet-f16-pilot-darpa-control/*, (2023-12-13).