For Japan, a Winning Formula is Cyber Defense and Innovation Offense

Krista Auchenbach
Senior Strategy Advisor, Office of the Secretary of Defense

Daniel Kliman
Senior Fellow, Center for a New American Security

Abstract

The already great and increasing importance of the cyber domain in strategic competition makes the need for Japan to advance its cyber-security and technology entrepreneurship development all the more pressing. Japan lags behind other major economies in this regard due to particular characteristics of its business environment and a lack of ways to develop talent for key cyber jobs. Coupled with Japan's aging population and competition from China, continued delay in addressing cyber and innovation concerns will lead to decreased competitiveness for the Japanese economy and military. However, Japan is in a unique position to leverage its existing public-private ties, already tech-savvy population, and the upcoming Tokyo Olympics to develop its cyber and entrepreneurial capacities.

Although Japan has the world's third largest GDP, it lags behind other major economies in both cyber-security and technology entrepreneurship.[1] With the cyber domain becoming a focal point for great power competition, inadequate defenses create national vulnerabilities that Japan's potential adversaries could use to coerce or hold its interests at risk. Japanese government and industry leaders have also identified an entrepreneurship deficit that constricts Japan's ability to evolve its economy to succeed given future technology trends and demographic headwinds.[2] To compete and prosper, Japan must embrace cyber-security and entrepreneurship—both of which underpin 21st century economic dynamism, and increasingly, technologies that support self-defense and military.

Why Japan Lags in Cyber-security and Entrepreneurship

Multiple factors account for Japan's lack of a cutting edge cyber-security capability and its comparative paucity of technology entrepreneurship.[3] From a structural perspective, business leadership has yet to fully appreciate the importance of cyber-security to corporate profitability.[4] Although this challenge is not unique to Japan, the more hierarchical nature of Japanese business reinforces the distance between corporate cyber-security units and company management.[5] Like many other economies, Japan has a shortage in cyber-security professionals and lacks ways to develop talent for key jobs.[6] Lastly, Japan is at the early stage of building linkages between government and industry around how to address cyber-security

---

[1] Mihoko Matsubara, "How Japan's New Cybersecurity Strategy Will Bring the Country Up to Par With the Rest of the World," June 4, 2018, https://www.cfr.org/blog/how-japans-new-cybersecurity-strategy-will-bring-country-par-rest-world.

[2] Ibid.

[3] "How to rev up Japanese startups," *The Economist,* November 16, 2017, https://www.economist.com/business/2016/11/05/how-to-rev-up-japanese-startups.

[4] Matsubara, "How Japan's New Cybersecurity Strategy Will Bring the Country Up to Par With the Rest of the World."

[5] Mihoko Matsubara, "Japan's cybersecurity must address gaps in loT and cloud security," (East Asia Forum, August 14, 2018), http://www.eastasiaforum.org/2018/08/14/japans-cybersecurity-must-address-gaps-in-iot-and-cloud-security/.

[6] Mihoko Matsubara, "How Japan Is Aiming to Close the Cybersecurity Skills Gap Before Tokyo 2020," Palo Alto Networks, May 15, 2017, https://researchcenter.paloaltonetworks.com/2017/05/cso-japan-aiming-close-cybersecurity-skills-gap-tokyo-2020/.

challenges, but is doing so with alacrity.[7] Indeed, the Japanese government has aptly recognized the opportunity that hosting the 2020 Summer Olympics provides as a society-wide forcing function to bolster Japan's cyber-security.[8]

Turning to entrepreneurship, Japan lacks a business ecosystem that is conducive to start-ups and fosters innovation outside major companies. Contrary to their American and European counterparts, many large Japanese companies continue to prefer that new hires become employees for life.[9] This makes it tough for aspiring entrepreneurs to leave established corporations to pursue their start-up aspirations, and return to the private sector if they fail. Even if their start-ups do succeed, large Japanese companies are often unwilling to source components from new firms, which threatens the viability of young companies.

Japanese companies have focused on providing excellent operations technology and hardware in their products. However, as the technology boom continues to transition to software-driven products, Japanese companies and government entities must increasingly focus on supply chain and other vulnerabilities that are inherent in software and internet connected devices.[10] To do so, government and industry definitions for "cyber-security" must be expanded to drive greater incident reporting—something companies are reluctant to do—and response, in order to better manage the risks associated with software-driven economies.[11] During our study tour to Japan with Sasakawa USA, several interlocutors noted a fear of processing personally identifiable information (PII) after a serious data breach. However, in order to enable entrepreneurial dynamism, Japan must address ways to enable PII protection in software development, and is now taking measures to do so.[12] A greater embrace of software development would also enable Japanese companies to expand their market outlook internationally.

---

[7] National Center of Incident Readiness and Strategy for Cybersecurity, *Summary of the Japan's Cybersecurity Strategy*, Cabinet Decision (July 2018), https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-zentaigaiyou-en.pdf.

[8] NHK World – Japan, "Japan draws up cybersecurity strategy," July 24, 2018, https://www3.nhk.or.jp/nhkworld/en/news/20180725_20/.

[9] "How to rev up Japanese startups," *The Economist.*

[10] Mina Pollmann, "Japan's Achilles Heel: Cybersecurity," *The Diplomat*, April 13, 2016, https://thediplomat.com/2016/04/japans-achilles-heel-cybersecurity/.

[11] Ibid.

[12] Nikkei Asian Review, "Japan to bar leak-prone IT providers from government contracts," August 20, 2018, https://asia.nikkei.com/Politics/Japan-to-bar-leak-prone-IT-providers-from-government-contracts.

Implications in a World of Strategic Competition

Japan's current lag in cyber-security and entrepreneurship incurs a real cost—one that is amplified by the growing strategic competition with China.[13]

Absent adequate cyber-security, Japanese companies may become less competitive over time due to cyber-enabled economic espionage, as their reliance on commercial off-the-shelf (COTS) software increases their vulnerability and Japan's hyper-connected internet of things economy expands its potential attack surface. As a result, there could also be significant vulnerabilities in Japanese critical infrastructure that could be held at risk during a crisis or conflict.

Without adequate technology entrepreneurship, Japan's economy is likely to become less dynamic in the coming decades given the demographic implications of an aging population. To offset a shrinking workforce, Japanese government and industry leaders are looking to commercial technology innovation to help provide future products and services to help supplant the loss of personnel.[14] This requires Japan to translate its enduring leadership in some scientific fields into new globally attractive commercial products. Entrepreneurship also extends to Japan's future self-defense and military edge. With technologies pioneered by startups increasingly relevant to national security,[15] the JSDF, just like any other military and security force, will need access to a homegrown innovation ecosystem to advance its capabilities. This is particularly salient given Japan's need to compete with China, whose businesses and military are well-along in leveraging the potential for civil-military fusion.[16]

---

[13] Michael Fitzpatrick, "Can Japan Reboot Its Anti-Innovation Start-up Culture?" August 21, 2013, *BBC*, http://www.bbc.com/future/story/20130820-plugging-japans-start-up-gap; and Japanese Ministry of Defense, *Defense of Japan* 2018, Annual White Paper (2018), http://www.mod.go.jp/e/publ/w_paper/pdf/2018/DOJ2018_Digest_0827.pdf.

[14] "Japanese businesses are struggling to keep up standards," *The Economist,* February 17, 2018, https://www.economist.com/business/2018/02/17/japanese-businesses-are-struggling-to-keep-up-standards.

[15] Dustin Volz, "Defense Secretary Mattis sees growth for Silicon Valley defense unit," Reuters, August 10, 2017, https://www.reuters.com/article/us-usa-cyber-mattis/defense-secretary-mattis-sees-growth-for-silicon-valley-defense-unit-idUSKBN1AQ2EB.

[16] Lorand Laskai, "Civil-Military Fusion and the PLA's Pursuit of Dominance in Emerging Technologies," (The Jamestown Foundation: China Brief, April 9, 2018), https://jamestown.org/program/civil-military-fusion-and-the-plas-pursuit-of-dominance-in-emerging-technologies/.

Opportunities for Japan

Japan can pair cyber defense with an innovation offense to strengthen its position in the strategic competition with China and sustain its economy. To do so, it must leverage a number of considerable national strengths. These include demonstrated excellence in hardware that could be applied to software design and cyber-security by building upon Japan's considerable strengths in basic research for key technology areas. Japan can also draw from its highly skilled, though admittedly thin, bench of experts to better deploy talent across its cyber-security workforce.[17] With a tech savvy population more willing to embrace robotics than most western societies,[18] Japan provides a fertile test ground to develop new technologies and applications across a spectrum of industries. Moreover, Japanese society has a comparatively high degree of trust among government, corporations, and society. This can support the necessary risk-taking that will be required to make progress in implementing the Japanese government's comprehensive strategy to mitigate its cyber-security shortfalls, particularly in the lead up to the 2020 Summer Olympics.

To kick-start its efforts, there are some measures Japan could take to improve its cyber-security and national entrepreneurship. These begin with better defining career paths for cyber-security professionals in government and industry to broaden experience and knowledge sharing. Next, the government can incentivize major Japanese corporations to enable and foster software development, source technology and ideas from start-ups, and expand into foreign markets. For example, Japan could leverage its trade and export promotion organization to help domestic start-ups open offices overseas at their outset in order to make them more competitive internationally.

Additionally, more extensive government-corporate cooperation could help bolster cyber-security standards, technology verification against supply chain and other vulnerabilities, and penetration testing to ensure critical infrastructure and key sectors are secure. A public-private talent development program could help foster commercial and government cyber workforces and capabilities that could rotate between government and industry, while also creating mechanisms to enable entrepreneurial efforts. For example, companies could institute "start-up sabbaticals" to create a method for employees to take time off to launch a start-up,

---

[17] Richard H. Ledgett, Jr., "Preparing for Cyber Attacks on Japan," *The Diplomat,* December 19, 2017, https://thediplomat.com/2017/12/preparing-for-cyber-attacks-on-japan/.

[18] "The growth of industrial robots," *The Economist*, March 27, 2017, https://www.economist.com/graphic-detail/2017/03/27/the-growth-of-industrial-robots.

while preserving a means to return to the company if the venture fails, and even developing shared equity agreements if the company succeeds.

Japan can thrive in a world of technology-centered strategic competition. But to do so, it must go from cyber-security laggard to leader, and build an economy conducive to start-up innovation.

Krista Auchenbach is Senior Strategy Advisor in the Office of the Secretary of Defense. Daniel Kliman is a Senior Fellow with the Asia-Pacific Security Program at the Center for a New American Security. *Both participated in a 2017 Sasakawa USA Emerging Experts Delegation to Japan focused on cyber-security and technology entrepreneurship. This commentary represents their personal views only and does not reflect upon the U.S. Government, the Department of Defense, the Secretary of Defense, or the Center for a New American Security.*