THE NATIONAL BUREAU
of ASIAN RESEARCH

COMMENTARY

Taiwan Sees Its Cyber Capabilities as the Hard Reality of Soft Power

BY BENSON WU

Published: August 24, 2017

The last decade has seen a paradigm shift in Taiwan regarding cyber capabilities. The influence of the mouse and keyboard on national security has increased substantially, and the government is further incorporating cyber as part of air, sea, and land operations.

Taiwan's focus on and investment in countering cyberattacks is unsurprising, as the island has become a front line for these types of attacks. In particular, Taiwan has been the target of a disproportionate number of cyberattacks for two main reasons. First, its political status and strategic position in the Asia-Pacific inevitably make the island a focal point of the region. Taiwan consistently attracts a variety of both large-scale and small cyberattacks. The first large-scale cyberattack occurred in 2003 and infiltrated several dozen government agencies and large private companies, making headline news and drawing significant public attention. In response, then cabinet spokesperson Lin Chia-lung reported that "national intelligence has indicated that an army of [state-sponsored] hackers…has successfully spread 23 different Trojan horse programs to the networks of 10 private high-tech companies here to use them as a springboard to break into at least 30 different government agencies and 50 private companies."[1]

These intrusions differed from traditional cyberattacks in that the intention was to steal sensitive or classified information rather than destroy critical systems. Over the past decade, security experts have concluded that there could be approximately seven to eight active state-sponsored malware campaigns, or so-called advanced persistent threats (APT), against Taiwan, targeting thousands of computers across a few hundred organizations, especially the 695 level A and level B government agencies, financial institutions (with 17 of the 38 targeted being ranked in the 2016 Forbes Global 2000), organizations responsible for critical infrastructure, and stock-exchange-listed high-tech companies.[2]

[1] Ko Shu-ling, "Cabinet Says Computers Under Attack," *Taipei Times*, September 4, 2003, http://www.taipeitimes.com/News/front/archives/2003/09/04/2003066387.

[2] Level A and level B organizations are those critical to the function and preservation of the state. Level A organizations include the Office of the President, the Five Yuan, and the governments of Taiwan's special municipalities, as well as government organizations or departments responsible for foreign policy, national and homeland security, the economy, critical infrastructure, and key public services, such as national health insurance, public records, and labor, among others. Level B organizations are county- and city-level governments and the relevant organizations at the local level that oversee social order and personal data information.

BENSON WU is an independent analyst. He has served in an advisory role with the Taiwan government on cyber and defense issues, as well in the private sector, and has participated and placed in hacker competitions. Mr. Wu is writing in his personal capacity and the views expressed in this commentary are his own and do not necessarily reflect the position of any organization with which he is affiliated.

Second, Taiwan has been investing significantly in its cyber infrastructure, both in terms of information technology and operational technology and by embracing new technologies like Industry 4.0, which includes automation, robotics, the "Internet of things," and financial technologies, to boost government efficiency and global competitiveness. With predominantly made-in-Taiwan products, global cybersecurity is linked directly with the island's supply chain security.

Such implications were witnessed in recent global cybersecurity crises. Stuxnet in 2010 and Duqu 2.0 in 2015 were controversial cyberattacks: though the weapons deployed differed, both attacks leveraged stolen digital certificates from world-leading Taiwan companies, namely RealTek Semiconductor, JMicron, and Foxconn, to gain access to computer systems under the guise of an authorized chipset supplier. This is increasingly becoming the norm in Taiwan as more and more Taiwan-based manufacturing giants are fighting hard against targeted attacks. Furthermore, the cyber heist in July 2016 of $2.5 million from the ATMs of one of Taiwan's leading banks once again demonstrated that there is much room for improving the island's overall cybersecurity measures.[3]

The current government, which assumed office in May 2016 and is led by President Tsai Ing-wen of the Democratic Progressive Party (DPP), is fully aware of these challenges and is determined to make improvements. Its approach includes three elements: legal, military, and civilian.

On the legal side, the newly established Department of Cyber Security under the Executive Yuan has drafted the Cyber Security Management Act that would require not only government agencies but also certain private companies to comply with cybersecurity policies and baselines. The act will set the standard for entities involved in eight major critical infrastructure areas—(1) energy, (2) water, (3) information and telecommunications, (4) transportation, (5) banking and finance, (6) emergency services and public healthcare, (7) central government, and (8) hi-tech industrial parks—and hold the relevant authority or business owner responsible and accountable for cyber breaches. Conversely, credits and awards will be granted for outstanding oversight.

In addition, the National Security Council is seeking support from the Legislative Yuan to refine the National Security Law so that what constitutes "digital territory" and "cyber operations" is clearly and appropriately defined. Taking the threats that the Government Service Network is encountering on a daily basis as an example, malicious or suspicious network connections around the island could be as high as a million per month. The revision should then lay the legal foundation to counteract these disturbances. The Tsai administration has appropriated a portion of its budget to meet these demands; cybersecurity-related programs (such as building cyber joint defense centers in six major cities) in the upcoming four years will receive around NT$9.5 billion (US$313 million) as part of the Executive Yuan's NT$1 trillion (US$32.35 billion) Forward-Looking Infrastructure Development Program that aims to boost Taiwan's economic growth.

The proposal on the military front is the formation of a fourth armed service that will assure Taiwan's cyber, communications, and electronic warfare capabilities, as outlined by the DPP in its Defense Policy Blue Paper.[4] On June 29, 2017, the new cyber unit comprising around six thousand personnel was formally launched as the Information, Communications and Electronic Force Command under the Ministry of National Defense. The promised budget includes NT$33 billion (around US$1.1 billion) in four years for system acquisition on proactive defense, infrastructure hardening, and cyber intelligence. While a significant portion of these capacities will be dedicated to cyber operations, a small number of select instructors (50–300) will

[3] "Taiwan Says Foreign Suspects Arrested over $2 million ATM Cyber Robbery," Reuters, July 17, 2016, http://www.reuters.com/article/us-taiwan-banks-theft-idUSKCN0ZX0N7.

[4] New Frontier Foundation, "Taiwan's Military Capacities in 2025," Defense Policy Blue Paper, no. 9, May 2015, 1, http://www.ustaiwandefense.com/tdnswp/wp-content/uploads/ 2014/12/20150526_DPP_Defense_Blue_Paper_9.pdf.

be responsible for skillset training and formalizing Taiwan's first-ever cyber operations manual. The planned systems will be developed primarily through indigenous production—e.g., the National Chung-shan Institute of Science and Technology is taking the initiative to build core systems and acquire niche components or advanced technologies from qualified Taiwan cyber companies. Another important factor will be international cooperation, especially with the United States and Israel. Among the systems, the overall motivation is to build a "cyber dome" over the island (analogous to Israel's Iron Dome) so that hostile operations are deterred at Taiwan's digital border. Civilian networks should no longer serve as the front line for country-level attacks.

Last, Taiwan's ethical hackers are renowned in the global security community for vulnerability hunting and operational team work. The local hacker community Hacks in Taiwan regularly participates in Defcon's Capture the Flag competition and finished second in 2014, fourth in 2015, fourth in 2016, and second in 2017. Interestingly, the Taiwan government has simultaneously worked to change the general public's perception of the hacker community. Now the government is aggressively supporting local cybersecurity communities, notably with President Tsai providing opening remarks at the Hacks in Taiwan conference in December 2016 and with the Ministry of Economic Affairs' Industrial Development Bureau granting funds to such ethical hacker events.[5] A few hacker groups have paved the way forward, founding start-ups (such as Xecure Lab for APT detection, T5 for threat intelligence, DevCore for high-quality penetration testing, and most recently CyCarrier for automated situation awareness) that tackle specific problems from a hacker's point of view and, in turn, sharing their in-depth findings with Black Hat, Defcon, or HITCON. Taiwan's government is working to streamline a national defense industry ecosystem between the fourth military unit, the National Chung-shan Institute of Science and Technology, and industry and community alliances to ensure that high-caliber talent can better contribute to Taiwan in the long run.

As the world enters an era of cyber asymmetries, small countries like Taiwan can do more for the world. Taiwan is keen to elevate its capabilities via international collaboration to better contribute to making the world safer. A good example of such capabilities would be implementing standards for the cyberdefense industry. In short, it is time for Taiwan to serve the world not only as a leader in high-tech manufacturing but also as a dependable partner in sharing cybersecurity intelligence and participating in joint cyber operations across the region. ~

[5] "Hackers Vie for US$10,000 Prize, Trip to Las Vegas," *Taipei Times,* December 3, 2016, http://www.taipeitimes.com/News/taiwan/archives/2016/12/03/2003660486.

THE NATIONAL BUREAU OF ASIAN RESEARCH (NBR) *is a nonprofit, nonpartisan research institution headquartered in Seattle, Washington, with a second office in Washington, D.C. For information on NBR's programs, please visit www.nbr.org.*

Media inquiries may be directed to Dan Aum at media@nbr.org or (202) 347-9767.

Join the NBR community: Facebook.com/NBRnews Twitter: @NBRnews