No 449 / June 2021

Facts & Findings

KONRAD ADENAUER STIFTUNG

Outward Defense

Comparing the Cyber Defense Postures of Japan, the Netherlands and the United States in Peace Time

Stefan Soesanto

- Targeted campaigns by adversarial nation state actors led to the evolution of cyber defense postures – their orientation ranges from more defensive to more offensive.

- Japan's defensively orientated approach focuses on hardening Japanese IT systems and increasing their resilience; the Dutch cyber defense posture is geared toward counter-intelligence efforts both at home and abroad to spoil adversarial campaigns; by conducting operations in adversarial networks the US strategy of persistent engagement proactively seeks to create friction within adversarial operations. Common to the three approaches is that the tasks of the military and (civilian) intelligence agencies overlap – the trend is toward organizational integration and joint operations.

- Currently none of the considered countries has found an effective and coherent approach to address all state sponsored malicious cyber activities yet. Therefore, continuous experimentation and a willingness to adapt and learn remains key to better defend the homeland in cyberspace.

Table of Contents

Background

Over the past decade, the question as to how a military is supposed to defend the nation in and through cyberspace during times of peace, has sparked an evolution of cyber defense postures across the globe, in which intelligence agencies often play a crucial role. While common to all these postures is the protection of the military's own networks and in some cases supporting mitigation efforts for serious incidents occurring in civilian networks – different geopolitical realities, risk perceptions, resource constraints, and other factors have created a diverse spectrum of increasingly diverging cyber defense postures. In light of the discussion on the alignment of cyber doctrines, i. e., whether it is necessary for states to proactively seize the initiative in cyberspace, this brief uses the defense postures of Japan, the Netherlands, and the United States, to exemplify their contrasting evolutionary pathways. By outlining their core guidelines, organizational background and operational conduct, the comparison of these three countries illustrates the spectrum from more defensive to more offensive postures. Lessons learned might be drawn from these cases to adapt, replicate, or create entirely new postures to defend the nation in and through cyberspace.

The Japanese Posture: Resilience and Non-engagement

Focus on resilience

The Japanese military is the most cautious and defensively orientated of the three countries. Spurred by a series of events in 2010, including (a) the discovery of Stuxnet; i. e., the joint US-Israeli offensive cyber operation against Iran's nuclear enrichment facilities; (b) heightened North Korean cyber activities against South Korean networks, and (c) the ramping up of Chinese cyber espionage efforts abroad, Tokyo decided to implement a wide-range of policies to build a resilient national cybersecurity posture at home.[1] While to date, Japan has not experienced any destructive cyberattacks against its critical infrastructure sectors, all of its major economic sectors have fallen victim to adversarial cyber espionage campaigns. Notably, in 2018, North Korean operatives also likely breached Japanese crypto-exchange *Coincheck*, stealing roughly $530 million USD.[2]

Constitutional constraints

On the offensive end, two elements inhibit Japan's cyber defense posture. On the one hand, Japan's intelligence community is still largely looking inward and lacks a strong mandate for foreign intelligence collection and espionage activities overseas. As a result, the Japanese National Police Agency is currently the most capable intelligence agency – focusing primarily on combating cybercrime, cyber terrorism, and cyber espionage. On the other hand, current governmental interpretations of Japan's constitution – which under Article 9 "forever renounces war" and "the threat to use force as a means of settling international disputes" – only allows the application of force for the purpose of self-defense. Meaning, offensive cyber operations are only permissible to "block and eliminate" an ongoing adversarial operation that fulfills the legal criteria of an armed attack.

To date, the Japanese Ministry of Defense (MoD) has not created a dedicated cyber command. Instead, a unit – known as the Cyber Defense Group – was stood up in 2013 with an envisioned 500 personnel, whose task is to "fundamentally strengthen [the Japanese Self-Defense Forces (SDF)] cyber defense capabilities, including capability to disrupt, in the event of attack against Japan, opponent's use of cyberspace for the attack as well as to conduct persistent monitoring of SDF's information and communications networks."[3] In 2012 and 2019 the MoD outsourced the development of offensive capabilities for the SDF to the Japanese private sector.[4] While the first developed "seek and destroy" malware was shelved for unknown reasons, the status of the second project is currently unknown.[5] As of this writing, neither the SDF, nor any of the numerous Japanese intelligence agencies, have conducted any known offensive cyber operations, nor any known cyber espionage campaigns against adversarial targets overseas. Within East Asia, this puts Japan on equal footing with Mongolia.

Importance of the US-Japan intelligence cooperation

Central to Japan's cyber defense posture is the US-Japan military alliance. Under the umbrella of US-Japan Cyber Defense Cooperation, multiple US and Japanese security and defense agencies closely cooperate on cyber threat intelligence sharing, capacity building, and military training exercises. However, given the current inability of the SDF to offensively operate in cyberspace, all efforts are currently geared toward hardening Japanese IT systems and enabling the SDF's computer emergency response teams to detect intrusions and remediate incidents as quick as possible (i. e., resilience). In April 2019, Washington and Tokyo officially proclaimed that "a cyber-attack could, in certain circumstances, constitute an armed attack for the purposes of Article V of the Japan-U.S. Security Treaty."[6]

The Dutch Posture: Intelligence Gathering and Counter-espionage

Intelligence collection & counter-intelligence

In 2009, the Dutch government embarked on a two-year long process to develop its first national cybersecurity strategy. In line with the strategy's envisioned principles, the Ministry of Defense published a document in late-2010 titled "the Vision of the military's cyber operations".[7] The document defines cyber operations as "operations or the defense against them, whereby a conscious effort is made to gather information and intelligence through infiltration of computers, computer networks, software and the Internet and to influence or disable systems in order to predict, influence or make impossible the actions of opponents."[8] The Military Intelligence and Security Service (MIVD) used the document to explore for the first time its role in cyber operations. The MIVD subsequently highlighted three cases in its annual report: Stuxnet, cyber espionage activities against NATO, as well as the coordinated Chinese Advanced Persistent Threat (APT) campaign against Google (Operation Aurora).[9] With the Dutch military being legally constraint from using offensive cyber operations during peace time, the focus almost naturally concentrated on intelligence gathering and counter-espionage efforts to: (a) be better informed about the origins and motivations of a cyberattack (attribution), identifying adversarial campaigns in their early stages (early warning), and gaining insights into the technical capabilities of potential adversaries (threat landscape).[10]

On the civilian end, the Dutch General Intelligence and Security Service (AIVD) within the Ministry of the Interior also started to move onto the topic of cyber espionage. Prior to 2010, all of the AIVD's annual reports merely mention cyber in the context of tackling cybercrime. But amidst the write up of the national cyber strategy, the AIVD began to emphasize the service's unique position to gain insights into cyber espionage, cyber terrorism, cyber extremism, and hacktivism.[11] Notably, the AIVD played a central role in the context of Stuxnet. It recruited the Iranian engineer who (a) provided crucial data for the targeted development of Stuxnet, and (b) had access to Iran's enrichment facility in Natanz to deploy Stuxnet onto the system using a USB flash drive.[12]

Joint forces

In 2011, the AIVD and MIVD subsequently commenced a pilot project that in the summer of 2014 culminated in the creation of the Joint Signal intelligence Cyber Unit (JSCU). The JSCU's purpose is to streamline the government's intelligence gathering and processing activities, as well as to bundle resources and personnel between both intelligence services.[13] The JSCU gained notoriety in January 2018, when the Dutch media reported that back in mid-2014, the JSCU successfully penetrated the computer network and security cameras of a building close to the Red Square in Moscow. At the time, Russia's Foreign Intelligence Service (SVR) used the building as their cyber operation headquarter.[14] According to *de Volkskrant*, the JSCU's intelligence collection efforts identified at least ten SVR cyber operatives, provided crucial evidence on Russia's interference in the 2016 US Presidential Election, and also forewarned the National Security Agency (NSA) of an SVR campaign against the networks of the US State Department.[15]

The MIVD was pushed into the public's eye in October 2018, when the Dutch Ministry of Defense decided to hold a press conference on the successful disruption of a close hacking operation against the Organisation for the Prohibition of Chemical Weapons (OPCW) six months prior.[16] Through the interception of four Russian military intelligence (GRU) officers, the MIVD was able to secure equipment and forensic data that revealed future GRU targets and past cyber espionage operations.[17] Among other items, the intelligence uncovered connected the GRU to the hack of the World Anti-Doping Agency and the US Anti-Doping Agency in 2016, and also crucially connected GRU officer Dimitry Badin to the 2015 Bundestag hack.[18]

Apart from these efforts, the Dutch government established a Defense Cyber Command (DCC) back in June 2015. With an envisioned personnel of 200, the DCC serves as a capability incubator whose mission is to develop offensive cyber capabilities that can be leveraged as force multipliers on the military battlefield.[19] Organizationally, the MIVD and JSCU substantially support the DCC by feeding it intelligence necessary for its defensive mission and to develop targeted exploits against adversarial military systems and infrastructure. As of this writing neither the DCC nor the Dutch intelligence services have officially conducted any offensive cyber operations against adversarial targets abroad.

The US Posture: Targeted Offensive Operations and Persistent Engagement

Threats below the threshold of an armed attack

The United States has been the victim of adversarial cyber espionage campaigns since at least 2002.[20] Notably, adversarial campaigns increased in the aftermath of Stuxnet, including the first destructive cyberattack against a US company in 2014 (Sand's Hotel and Casino), the exfiltration of private information of 21.5 million former, current, and prospective government employees in 2015 (OPM hack), and the interference in the US Presidential Election in 2016 (DNC hack). [21] By 2017, the Department of Defense's (DoD) Defense Science Board soberly concluded that "the unfortunate reality is that, for at least the coming five to ten years, the offensive cyber capabilities of our most capable potential adversaries are likely to far exceed the United States' ability to defend and adequately strengthen the resilience of its critical infrastructures."[22]

Change of strategy

Established in 2010, US Cyber Command (USCC) is the DoD's unified combatant command in the cyber domain. Headquarter at Fort Meade and dual-hatted – meaning, the commander of USCC is also the director of the National Security Agency (NSA) – USCC oversees 12,000 personnel, four service cyber components, and 133 Cyber Mission Force teams consisting of 6,000 service members.[23] Yet, despite its size and strength, USCC was unable to defend the nation because the adversarial campaigns remained below the legal threshold of an armed attack. Responding to these inadequacies, USCC officially endorsed the strategy of persistent engagement (PE) in 2018.[24] PE is based on the observation that deterrence and operational restrain in cyberspace are not a credible strategy, because cyberspace is an environment of constant contact. With targeted cyber operations in adversarial networks, PE therefore aims to operate globally, seamlessly, and continuously, to persistently create friction within adversarial operations.[25]

Imposing costs and friction on adversaries

To date, the tactical implementations of PE have been rather diffuse. On the one hand, tools include the deployment of hunt forward teams to NATO's eastern periphery for intelligence collection purposes, and the public sharing of adversarial malware samples to burn adversarial tooling.[26] On the other hand, USCC pre-emptively ran an offensive cyber operation that temporarily took out the Internet Research Agency, a Kremlin-linked troll farm, in the run-up to the 2018 mid-term elections.[27] And in 2020, USCC cooperated with Microsoft in an attempt to take down Trickbot – "one of the world's most infamous botnets and prolific distributors of malware and ransomware" – to defend the 2020 US Presidential election and disrupt the wave of ransomware campaigns against US infrastructure amidst the Covid-19 pandemic.[28] According to the commander of USCC, Gen. Nakasone, USCC "conducted more than two dozen operations to get ahead of foreign threats before they interfered with or influenced our elections in 2020."[29] Despite, or rather, because of these limited efforts, the strategy of persistent engagement has come under intense scrutiny for not having detected nor prevented the SVR's supply chain attack against Solarwinds.

Tactical implementations of persistent engagement

It remains to be seen what lessons learned USCC will take away from this massive intelligence failure, and whether the Biden administration has the political appetite toward enhancing visibility in adversarial networks and accelerate persistent engagement toward truly operating globally, seamlessly, and continuously against adversarial operations wherever they maneuver.

Conclusion: Further Need of Experimentation and Adaptability

The three cyber defense postures outlined differ vastly from each other in both the resources dedicated and the outcomes produced. What the three approaches have in common is that the tasks of the military and (civilian) intelligence agencies in cyberspace overlap and the trend is toward organizational integration and joint operations.

The Japanese approach is largely shaped by its constitutional constraints and the absence of a large intelligence agency specifically dedicated to foreign intelligence collection. As such, Tokyo's passiveness and focus on homeland defense in cyberspace, follows its defense posture in real space. To break with this conundrum, Japan's overall defense strategy would likely have to change and overwrite its constitutional constraints. One pressure point that might facilitate such a change could be if the US loses confidence in Japan as a reliable ally, as Tokyo continues to fall victim to Chinese espionage campaigns and remains unable to develop and leverage offensive cyber capabilities to carry its share of the alliance's burden in cyberspace.

Risk of erosion of confidence

In contrast to Japan, the Dutch defense posture is by design geared toward counter-intelligence efforts both at home and abroad to spoil adversarial campaigns. The primary objective of the MIVD and AIVD is to clear up intelligence blind spots and potentially open up new insights in adversarial activities. To some degree, one could argue, that the Dutch intelligence agencies actually practiced elements of persistent engagement by pure coincidence when they breached the network at the SVR's hideout at the Red Square. Some of the intelligence gathered is actionable to better defend the Netherlands, while other

Unclear role of the military

pieces might be shared with allies if deemed relevant and appropriate. The problem with the Dutch approach is that DCC is largely left out of this loop and remains highly dependent upon the MIVD's intelligence sourcing. As such, it is unclear what the DCC is currently capable of, and whether it can reliably develop specific tooling against designated military targets ahead of time. At present DCCs capabilities, mandate, and size make it one of the smallest cyber commands in the world.

Risk of escalation?

The US cyber defense posture is vastly more expansive than what the Dutch have been practicing. Conceptually, one might even argue that the aspiration of persistent engagement will naturally veer toward adversarial containment and an even higher drumbeat of offensive cyber operations over time. To a large degree, geopolitical developments in real space and an increasing threat environment in cyberspace go hand in hand with shaping the US defense posture. As of this writing, there are no feasible strategic alternatives for the US that might replace persistent engagement. It even remains to be seen whether the US cyber defense posture will be replicated elsewhere. So far, the Japanese government has not voiced the slightest interest in discussing PE in any way shape or form. Similarly, in the Netherlands, PE is viewed as too resource intense and potentially escalatory to be adopted in the European context.

Time will tell which of the three defense postures is better equipped to handle an ever-changing threat landscape and can adequately balance risks and resources in the years ahead. While no cyber defense posture is perfect, continuous experimentation and a willingness to adapt and learn remains key to better defend the homeland in cyberspace.

[1] Stefan Soesanto, “Japan’s National Cybersecurity and Defense Posture – Policy and Organizations”, 09.2020, Center for Security Studies/ETH Zurich, retrieved 28.02.2021 from: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-08-Japans-national-cybersecurity-defense-posture.pdf, p. 11.

[2] Deutsche Welle, “Japanese authorities raid Coincheck headquarters”, 02.02.2018, Deutsche Welle, retrieved 28.02.2021 from: https://www.dw.com/en/japanese-authorities-raid-coincheck-headquarters/a-42418654; Michelle Nichols, “North Korea took $2 billion in cyberattacks to fund weapons program: U.N. report”, 05.08.2019, Reuters, retrieved 10.05.2021 from: https://www.reuters.com/article/us-northkorea-cyber-un-idUSKCN1UV1ZX.

[3] Ministry of Defense, “Medium Term Defense Program (FY 2019 - FY 2023)”, 18.12.2018, Mod.go.jp, retrieved 28.02.2021 from: https://www.mod.go.jp/j/approach/agenda/guideline//pdf/chuki_seibi31-35_e.pdf, p. 3.

[4] John Leyden, “Japan tasks Fujitsu with creating search-and-destroy cyber-weapon”, 03.01.2012, The Register, retrieved 28.02.2021 from: https://www.theregister.co.uk/2012/01/03/japan_cyber_weapon_research/.

[5] The Japan Times, “In first, Japan to develop computer virus to defend against cyberattacks “, 30.04.2019, The Japan Times, retrieved 28.02.2021 from: https://www.japantimes.co.jp/news/2019/04/30/national/first-japan-develop-computer-virus-defend-cyberattacks/#.XmDjcKhKhaQ.

[6] Ministry of Defense, “Joint Statement of the Security Consultative Committee”, 19.04.2019, retrieved 10.05.2021 from: https://www.mod.go.jp/e/d_act/us/201904_js.html.

[7] Bertelink, Becx, Bijl, Boogaard, Campenhout, Le Clercq, Havinga, Kooij, Veenendaal, Vos, “Visie op Defensie cyber operations”, 2010, Ministerie van Defensie.

[8] Ibid., p. 14 (Google translate), in D.A. Dreijer, “Offensieve Cyberoperaties. Een onderzoek naar de fasering en uitvoering van offensieve cyberoperaties die plaatsvinden in de context van een internationaal conflict“, retrieved 17.05.2021 from: https://www.nlda-tw.nl/janmartin/vakken/TIOP/Cyber%20Warfare/Offensieve%20cyber%20operaties%20versie%2014032011%20definitief%20DA%20Dreijer.pdf, p. 16.

[9] Militaire Inlichtingen- en Veiligheidsdienst (MIVD), “Jaarverslag 2010“, Ministerie van Defensie, retrieved 28.02.2021 from: https://www.inlichtingendiensten.nl/militair/jaarverslagmivd2010.pdf, p. 50.

[10] Ibid., p. 62.

[11] Algemene Inlichtingen- en Veiligheidsdienst (AIVD), “Jaarverslag 2010“, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, retrieved 28.02.2021 from: https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2011/04/20/jaarverslag-aivd-2010/jaarverslag_2010_pdf_versie.pdf, p. 26.

[12] Kim Zetter und Huib Modderkolk, “Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran“, 02.09.2019, YahooNews, retrieved 28.02.2021 from: https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html.

[13] Ministerie van Defensie, „Ontdek de Joint SIGINT Cyber Unit van de MIVD“, werkenbijdefensie.nl, n.d., retrieved 28.02.2021 from: https://werkenbijdefensie.nl/joint-sigint-cyber-unit-mivd.

[14] As the current narrative goes, the JSCU appears to have stumbled upon the SVR’s hideout by pure coincidence as they were reverse engineering a malware payload and connected command-and-control servers (see Florian Flade, Hakan Tanriverdi, “Der Mann in Merkels Rechner – Jagd auf Putins Hacker - #5 Hackback“, 22.04.2021, BR Podcast, retrieved 30.04.2021 from: https://www.br.de/mediathek/podcast/der-mann-in-merkels-rechner-jagd-auf-putins-hacker/5-hackback/1823407, timestamp: 1:30-3:43).

[15] Huib Modderkolk, “Dutch agencies provide crucial intel about Russia’s interference in US-elections”, 25.01.2018, De Volkskrant, retrieved 28.02.2021 from: https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/.

[16] Ministerie van Defensie, “Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW”, 04.10.2018, english.defensie.nl, retrieved 28.02.2021 from: https://english.defensie.nl/latest/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw.

[17] Ministry of Defence, “GRU close access cyber operation against OPCW. Genmaj. O. Eichelsheim”, 04.10.2018, english.defensie.nl, retrieved 10.05.2021 from: https://english.defensie.nl/binaries/defence/documents/publications/2018/10/04/gru-close-access-cyber-operation-against-opcw/ppt+pressconference+ENGLISH+DEF.pdf.

[18] The United States Department of Justice, „U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations”, 04.10.2018, US Department of Justice, retrieved 28.02.2021 from: https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and; Florian Flade, Georg Mascolo, “Bärenjagd”, 05.05.2020, Süddeutsche Zeitung, retrieved 28.02.2021 from: https://www.sueddeutsche.de/politik/hack-bundestag-angriff-russland-1.4891668.

[19] Liza van Lonkhuyzen, Kees Versteegh, “Het cyberleger kan en mag nog weinig“, 18.12.2018, NRC, retrieved 28.02.2021 from: https://www.nrc.nl/nieuws/2018/12/18/het-cyberleger-is-er-wel-maar-mag-weinig-a3099254.

[20] Stefan Soesanto, “The Evolution of US Defense Strategy in Cyberspace (1988–2019)”, 08.2019, Center for Security Studies/ETH Zurich, retrieved 28.02.2021 from: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-The-Evolution-of-US-defense-strategy-in-cyberspace.pdf, p. 10.

21 Robert S. Mueller, “Report On The Investigation Into Russian Interference In The 2016 Presidential Election”, 03.2019, US Department of Justice, retrieved 28.02.2021 from: https://www.justice.gov/archives/sco/file/1373816/download, p. 38 ff.

22 Department of Defense, Defense Science Board, “Task Force on Cyber Deterrence”, February 2017, United States Senate Committee on Armed Services, retrieved 10.05.2021 from: https://www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf, p. 4.

23 U.S. Cyber Command, “Executive Director. USCYBERCOM. Dave Frederick”, n.d., U.S. Cyber Command, retrieved 10.05.2021 from: https://www.cybercom.mil/About/Leadership/Bio-Display/Article/1651709/executive-director-uscybercom/.

24 Note: US Cyber Command’s Operation Glowing Symphony against the Islamic State’s propaganda unit does not fall under persistent engagement. For more about the operation see: Dina Temple-Raston, “How The U.S. Hacked ISIS”, 26.09.2019, NPR, retrieved 28.02.2021 from: https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

25 Richard Harknett und Emily Goldman, “The search for cyber fundamentals”, Journal of Information Warfare, Vol. 15, Issue 2, retrieved 28.02.2021 from: https://www.jinfowar.com/journal/volume-15-issue-2/search-cyber-fundamentals; Michael Fischerkeller und Richard Harknett, “Deterrence is not a credible strategy for cyberspace”, 2017, Orbis, Vol. 61, Issue 3, retrieved 28.02.2021 from: https://www.sciencedirect.com/science/article/abs/pii/S0030438717300431.

26 Mark Pomerleau, “How ‘hunt forward’ teams can help defend networks”, 12.02.2020, Fifth Domain, retrieved 28.02.2021 from: https://www.fifthdomain.com/dod/2020/02/12/how-hunt-forward-teams-can-help-defend-networks/; Catalin Cimpanu, “US Cyber Command starts uploading foreign APT malware to VirusTotal”, 08.11.2018, ZDNet, retrieved 28.02.2021 from: https://www.zdnet.com/article/us-cyber-command-starts-uploading-foreign-apt-malware-to-virustotal/.

27 Julian E. Barnes, “Cyber Command Operation Took Down Russian Troll Farm for Midterm Elections”, 26.02.2019, The New York Times, retrieved 28.02.2021 from: https://www.nytimes.com/2019/02/26/us/politics/us-cyber-command-russia.html.

28 Ellen Nakashima, “Cyber Command has sought to disrupt the world’s largest botnet, hoping to reduce its potential impact on the election“, 10.10.2020, The Washington Post, retrieved 28.02.2021 from: https://www.washingtonpost.com/national-security/cyber-command-trickbot-disrupt/2020/10/09/19587aae-0a32-11eb-a166-dc429b380d10_story.html; Microsoft, “Microsoft takes action to disrupt botnet and combat ransomware”, 13.10.2020, Microsoft.com, retrieved 30.04.2021 from: https://news.microsoft.com/apac/2020/10/13/microsoft-takes-action-to-disrupt-botnet-and-combat-ransomware/.

29 Paul Nakasone, “Posture Statement of General Paul M. Nakasone, Commander, United States Cyber Command before the 117th Congress Senate Armed Services Committee – March 25, 2021”, 25.03.2021, Senate Armed Services Committee, retrieved 30.04.2021 from: https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-25-21.pdf, p. 3.

Imprint

The Author

Stefan Soesanto is a Senior Researcher in the Cyberdefense Project with the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zurich.

Konrad-Adenauer-Stiftung e. V.

Johannes Wiggen
Policy Advisor on Cybersecurity
Analysis and Consulting
T +49 30 / 26 996-3934
johannes.wiggen@kas.de

Postal address: Konrad-Adenauer-Stiftung, 10907 Berlin

This publication of the der Konrad-Adenauer-Stiftung e. V. is solely intended for information purposes. It may not be used by political parties or by election campaigners or supporters for the purpose of election advertising. This applies to federal, state and local elections as well as elections to the European Parliament.

Publisher: Konrad-Adenauer-Stiftung e. V. 2021, Berlin
Design: yellow too, Pasiek Horntrich GbR
Typesetting: Janine Höhle, Konrad-Adenauer-Stiftung e. V.

Produced with financial support from the German Federal Government.

ISBN 978-3-95721-935-0