The Heritage Foundation

BACKGROUNDER

No. 3711 | MAY 31, 2022

Opportunities Abound for Further U.S.–South Korean Cyber Cooperation

Dustin Carmack and James Di Pane

KEY TAKEAWAYS

The U.S. and South Korea have both made tangible improvements on their cybersecurity cooperation and their respective cyber policies.

But the U.S and South Korea still have much work to do in deterring the pre-eminent global cyber threat—the Chinese regime.

President Joe Biden should focus on increasing strategic cyber cooperation with South Korea at a time of increasing global instability and cyber threats.

President Biden just returned from a three-day trip to South Korea, at a time of increasing tensions on the Korean Peninsula and the inauguration of a new South Korean president, Yoon Suk-yeol.[1] The importance of maintaining the strong bilateral and historical relationship with South Korea offers opportunities not only to increase mutual security and military alliance issues as they relate to North Korean nuclear and ballistic missile provocations, but also as they relate to the broader Indo–Pacific cyber environment.[2]

Going forward, President Biden should focus on increasing cyber cooperation with President Yoon's government at a time of increasing global instability and cyber threats emanating not only from North Korea, but from China, Iran, Russia, and criminal actors seeking to infiltrate critical infrastructure and weaponize lucrative financial attacks on digital currency exchanges.

The United States' and South Korea's global roles in technology, and lessons about the development of various cyber defenses and policies, offer an opportunity for both sides to learn from the other's successes and failures and build an enduring and strong cyber posture.

An Evolving Cyber Relationship

The United States and South Korea have developed separate and joint cyber policies and cyber capabilities over the past 15 years. The U.S. formally established Cyber Command in the second year of the Obama Administration, and South Korea laid out its first cyber strategy in 2009. Both sides have been active participants and leaders in the international arena as the world rapidly digitized and cyber borders became increasingly porous, and, hence, vulnerable to a variety of threats from both nation-states and criminal actors.

South Korea has made cyber policy changes primarily in response to cyberattacks against it, as well as due to evolving threats.[3] Many of these began as distributed denial of service (DDoS) attacks, while intelligence-gathering operations have evolved to include malicious malware; penetration of critical infrastructure facilities, such as nuclear plants and hydropower dams; ransomware; and the pillaging and laundering of digital currencies to fund illicit operations and avoid international sanctions. In 2015, South Korea appointed its first cyber adviser who answered to the president and South Korea's National Security Council after a spate of attacks in 2013 and 2014.

Similarly, the United States has made significant changes after attacks, such as North Korea's hacking of the Sony Pictures network, which inflicted major financial damage on the company. Most recently, in light of a range of recommendations from the Cyberspace Solarium Commission, the U.S. has implemented vast policy changes, including the creation of the nation's first National Cyber Director position to coordinate overall government cyber strategy, including broadening engagement and information sharing within the private sector with varying federal agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), and Federal Bureau of Investigation (FBI). The 2021 ransomware attack on Colonial Pipeline led to the creation of cyber-incident-disclosure-reporting requirements for critical infrastructure operators.[4]

Much of the focus on cybersecurity and concerns at the national level revolve around threats to critical infrastructure. For example, more than 80 percent of the U.S. energy infrastructure is owned and operated by the

private sector.[5] South Korea is nearly the opposite in that regard. It is estimated that more than 70 percent of South Korea's critical infrastructure facilities are owned by the public sector and governed by the National Cyber Security Center.[6]

Recent Developments

Both the Trump and Biden Administrations pledged to further the U.S. cyber relationship with South Korea. South Korea faced a range of cyberattacks emanating from China and Russia leading up to the 2018 U.S.–North Korea summit.[7] In 2019, the 51st Republic of Korea–United States Security Consultative Meeting led to commitments by both countries to ensure joint response capabilities against cyber and space threats. President Biden's bilateral meetings with former South Korean President Moon Jae-in resulted in the creation of a cybersecurity working group to enhance law enforcement cooperation; prevent and, if necessary, mitigate, ransomware attacks; and implement lessons learned from previous cybercrimes in both countries.[8] Additionally, the two countries established a joint working group focused on cyber-exploitation to "end the abuse of women online and offline" and the financing of online sexual exploitation.

The emergence of COVID-19 led to the "Korean New Deal" in 2020, which included a "Digital New Deal," as much of the country worked remotely. The Korean government heavily promoted sub-projects, including on fifth-generation (5G) wireless technology, artificial intelligence, blockchain technology, and cloud-computing technology, with a focus on advancing cybersecurity.[9]

In recent years, the global proliferation of ransomware has had adverse impacts on both countries and led to government efforts to engage public-sector and private-sector entities on defense mechanisms and sanctions, indictments, and international cooperation.[10] FBI Director Christopher Wray noted that U.S. ransomware victims paid an estimated $350 million in ransom in 2020, and that the number of complaints the FBI received increased by 82 percent between 2019 and 2021.[11]

The U.S. Department of Justice (DOJ) indicted three North Korean military hackers in 2021 for a wide-ranging criminal conspiracy to conduct a series of destructive cyberattacks, to steal and extort more than $1.3 billion of money and cryptocurrency from financial institutions and companies, to create and deploy multiple malicious cryptocurrency applications, and to develop and fraudulently market a blockchain platform.[12]

Additionally, the DOJ created a National Cryptocurrency Enforcement Team (NCET) alongside the FBI's creation of a Virtual Asset Exploitation Unit, specifically focused on disrupting cybercrime and international virtual currency used in such crimes.[13] The goal of the program is to help law enforcement authorities in other countries to "improve their techniques and abilities in cryptocurrency investigations."[14]

In May 2022, the U.S. Department of the Treasury announced the sanctioning of an online cryptocurrency mixer for its ties to the North Korean Lazarus Group and its use of the mixer to launder more than $20 million of a recent $620 million heist by the group.[15]

The U.S. and South Korea have recently participated in several international cyber exercises of note. The North Atlantic Treaty Organization's (NATO's) Locked Shields exercise, hosted by the NATO Cooperative Cyber Defense Center of Excellence (CCDOE) in Estonia, is the world's largest annual interactive cyber drill and includes more than 2,000 participants from 32 countries.[16] South Korea has participated in the exercise since 2018, and after its most recent participation in April 2022, was officially admitted as a contributing participant to the CCDOE.[17] A commentator for *The Global Times*, the Chinese Communist Party state media apparatus, tweeted a not-so-veiled threat against South Korea after South Korea's admittance: "If South Korea takes a path of turning hostile against its neighbors, the end of this path could be a Ukraine."[18]

Although North Korea will brazenly continue to use its cyber capabilities to achieve a variety of goals, China is the pre-eminent global cyber threat. U.S. Director of National Intelligence Avril Haines testified recently that China "presents the broadest, most active, and persistent cyber espionage threat to U.S. government and private sector networks."[19]

Strengthening Cyber Cooperation

President Yoon campaigned on the renewal of a "comprehensive strategic alliance" with the United States. While the U.S. and South Korea have made tangible improvements on their cybersecurity cooperation and their respective cyber policies, there is room for strategic improvement and a need for expeditious results.

The Biden Administration should:

- **Strengthen the relationship between law enforcement entities, including the DOJ's NCET and the FBI's Virtual Asset Exploitation Unit.** The U.S. should use these units to further international collaboration

on reducing cybercrime. The DOJ will send a cyber-operations liaison to Europe to work with Eurojust,[20] the European Union judicial cooperation and joint investigation agency, on accelerating cases against top cybercriminals.[21] An appointment of such an official would be useful in the Indo–Pacific, too, with the U.S. embassy in Seoul possibly being a prime location for housing such expertise.

Yoon's presidential election campaign focused significantly on the future of cryptocurrency and South Korean leadership on technology issues. Immense challenges and opportunities have arisen with blockchain technology and cryptocurrencies. Any regulatory approaches must be evenly balanced and not impede future capabilities in these emerging fields.[22] Law enforcement must investigate, prosecute, and sanction the exploitation of cryptocurrency exchanges for criminal and financial means. The two countries have much to offer in maximizing the benefits of digital currency while increasing resources and expertise to combat nefarious uses, including North Korea's predominant usage of funding illicit operations and avoiding sanctions. Both countries must fully enforce laws and sanctions against North Korea and other malicious cyber actors who provide technology, equipment, or training to North Korea.[23]

- **Engage in "defend forward" operations.** The U.S. should increase the number of forward deployed cyber teams in South Korea and use them to enhance the "defend forward" posture of both governments. In 2018, the U.S. planned to establish a cyber planning cell in South Korea to address the threat from North Korea.[24] Known as a cyber-operations integrated planning element (CO-IPE), the planning cell's primary purpose is to help U.S. and allied military leaders to coordinate cyber tools with the more traditional military forces like air and ground troops. U.S. Forces Korea was the first sub-unified combatant command to receive such a team. The U.S. and South Korea should expand and enhance this team to strengthen its ability to respond to North Korean and Chinese cyber operations. In addition, the U.S. and South Korea should apply lessons learned from recent defend forward operations, like those in Europe supporting Ukraine, to help the alliance adopt best practices for responding to and deterring threats in cyberspace.[25] In his April testimony before the U.S. Senate Armed Services Committee, General Paul Nakasone, Commander of U.S. Cyber Command and NSA Director, explained how the deployment of "hunt

forward" teams to support Ukraine helped in securing both Ukrainian and U.S. cyber networks and strengthened the homeland defense of both countries. This operational experience provides lessons that the U.S. could apply to working with other allies.[26] The U.S. and South Korea should apply these lessons from the ongoing war in Ukraine, and from persistent engagements with Russia and other adversaries seeking to create mayhem, to enhance cooperation and deterrence.[27]

- **Invite South Korean participation in Quad Senior Cyber Group and Quad Plus cyber engagements.** At last year's Quad summit, the four members (Australia, India, Japan, and the United States) agreed on the creation of a Quad Senior Cyber Group to advance "shared cyber standards; development of secure software; building workforce and talent; and promoting scalability and cybersecurity of secure and trustworthy digital infrastructure."[28] The Quad should invite South Korea to future cyber engagements as an observer or as part of broader Quad Plus engagements.[29] These five countries have an immense role in the future of Indo–Pacific security as well as technological development and standards.[30]

The Biden and Yoon Administrations should:

- **Study critical infrastructure regulatory lessons and warnings.** The U.S. and South Korea can benefit from regulatory lessons about protecting critical infrastructure. As much of the world has similarly seen, cyberattacks against South Korean networks are increasing, while *damages* from such attacks are decreasing.[31] The U.S. must move forward expeditiously to properly define critical infrastructure and implement the recently passed mandatory cyber-incident-disclosure law. South Korea may offer unique lessons to the U.S. on what has worked well within its regulatory apparatuses as it relates to critical infrastructure and vice versa. Both countries must avoid overly burdensome and one-size-fits-all regulations, with the end goal of building resilient cyber defenses that have the capability to identify and quickly remediate cyberattacks.[32]

- **Increase joint operational exercises.** The U.S. and South Korea should increase the frequency and quality of cybersecurity exercises to include live-fire exercises on both the military and homeland security levels. Exercises are an excellent tool for strengthening interoperability

and communication, as well as for testing doctrine. These exercises should focus specifically on resilience, backup systems, and being persistently engaged with prolific actors like North Korea and China. The U.S. and South Korea should continue working within the NATO CCDOE[33] framework to allow coordination with a large number of allies to gain military cyber experience, as well as identifying homeland security partners, such as CISA's Joint Cyber Defense Collaborative (JCDC) and the NSA's Cybersecurity Collaboration Center, for a focus on critical infrastructure and domestic network defense.[34]

- **Impose costs on malicious actors.** The U.S. and South Korea should do more to impose costs on malicious cyber actors like China and North Korea. Historically, South Korea has been aggressive in attributing North Korean cyberattacks but has not identified similar attacks from Russia and China. Identifying these countries when they conduct cyberattacks is an important tool for building international pressure on them as a means of deterring this type of activity. In addition, it is important not to rely solely on strengthening cybersecurity and the resilience of networks, but to also employ a robust offensive capability and forward defense as a means of strengthening deterrence. In cyberspace, the advantage often goes to the aggressor, so a strategy based on reaction and defense alone is doomed to fail against a persistent adversary.

- **Cooperate further on transportation and operational technology cybersecurity.** The U.S. Department of Homeland Security recently announced cooperation with South Korea on airport-security screening software to assist the U.S. Customs and Border Protection and the Transportation Security Administration. The U.S. and South Korea should expand research and development for cyber defenses as it relates to operational technology (OT) and industrial control systems (ICS).[35] Commercial critical infrastructure and transportation systems, such as energy production and pipelines, water and waste management, airlines, and passenger and freight rail, all rely heavily on OT platforms that continue to be targets of North Korea and other bad actors, such as China, Iran, and Russia. Within existing U.S. Department of Energy research programs, the U.S. and South Korea should study grid reliability and cooperate on building capabilities for black-start recoveries. The two countries should also extend research into collaboration on cyber-defense-weapons-systems security.

- **Engage international partners and structures.** South Korea's recent engagements and growing relationships with NATO and work on broader international cyber standards are helpful. In addition to encouraging Seoul to participate in Quad Plus dialogues, Washington should encourage Seoul to continue its ongoing bilateral cooperation with cybersecurity allies Australia,[36] Israel,[37] Japan,[38] and the United Kingdom.[39]

To date, South Korea has not signed the Budapest Convention on Cybercrime, which is the primary mechanism for many nations to cooperate on cybercrime investigations.[40] Participating countries held discussions in late 2021 on possible updates to the Budapest Convention to further assist law enforcement agencies in gaining access to data outside their jurisdictions. Under a revised convention, "new legal channels would make it easier for prosecutors and police to obtain digital evidence quickly by directly contacting technology companies outside their jurisdiction."[41] The DOJ just signed the updated Second Additional Protocol to the Budapest Convention in May. According to the DOJ, the updated convention is

> specifically designed to help law enforcement authorities obtain access to such electronic evidence, with new tools including direct cooperation with service providers and registrars, expedited means to obtain subscriber information and traffic data associated with criminal activity, and expedited cooperation in obtaining stored computer data in emergencies. All these tools are subject to a system of human rights and rule of law safeguards.[42]

While Washington should encourage Seoul to continue to consider accession to the Budapest Convention and give feedback to any updates to the convention that may be agreed upon this year, bilateral agreements between U.S. and South Korean law enforcement entities should proceed without delay, regardless of whether South Korea joins the convention. The U.S. and South Korea should be clear eyed about the limitations of the Budapest Convention, given that malicious cyber actors, such as China, Iran, North Korea, and Russia, will never play by the rules. Nevertheless, the convention remains a forward-leaning tool that can assist in broader cybercrime cases and facilitate efficient information sharing.

Conclusion

President Biden's trip to South Korea provides an opportunity to continue the forward momentum that has developed on broader cybersecurity cooperation in the Indo–Pacific and with South Korea. Silver-bullet solutions for a constantly evolving cyber environment do not exist. There are, however, many lessons from both sides of the Pacific as both countries continue to develop layered cyber-defense apparatuses, and as they seek to deter and impose costs on foreign cyber adversaries and criminal groups, especially those in China and North Korea.

Reducing any bureaucratic barriers to protection of intellectual property and export licensing should also be a priority for the Biden Administration in order to strengthen the broader U.S.–South Korea relationship.

These steps can provide a footing not only to challenge security threats in the Korean Peninsula emanating from North Korea, but also near-term and long-term threats from China's cyber and technological tentacles that seek to restrict freedom within the broader Indo–Pacific and the world.

Dustin Carmack is Research Fellow for Cybersecurity, Intelligence, and Emerging Technologies in the Border Security and Immigration Center at The Heritage Foundation; and **James Di Pane** is Policy Analyst for Defense Policy in the Center for National Defense at The Heritage Foundation.

Endnotes

1. Alex Leary, "Biden to Visit South Korea, Japan in May," *The Wall Street Journal*, April 27, 2022, https://www.wsj.com/articles/biden-to-visit-south-korea-japan-in-may-11651110521 (accessed May 11, 2022), and "Biden Pushes Economic and Security Aims as He Ends Visit to South Korea," CBS News, May 22, 2022, https://www.cbsnews.com/news/biden-south-korea-economic-security-aims/ (accessed May 23, 2022).
2. Bruce Klingner and Jeff M. Smith, "President Biden Should Strengthen Alliances During Asia Trip," Heritage Foundation *Issue Brief* No. 5268, http://report.heritage.org/ib5268.
3. So Jeong Kim and Sunha Bae, "Korean Policies of Cybersecurity and Data Resilience," in Evan A. Feigenbaum and Michael R. Nelson, eds., *The Korean Way With Data: How the World's Most Wired Country Is Forging a Third Way* (Washington, DC: Carnegie Endowment for International Peace, 2021), https://carnegieendowment.org/2021/08/17/korean-policies-of-cybersecurity-and-data-resilience-pub-85164 (accessed May 6, 2022).
4. Brian Stone, "One Year Removed from the Colonial Pipeline Attack, What Have We Learned?" *TechRepublic*, May 6, 2022, https://www.techrepublic.com/article/one-year-colonial-pipeline-attack-learned/ (accessed May 12, 2022).
5. Cybersecurity and Infrastructure Security Agency, "Energy Sector," https://www.cisa.gov/energy-sector#:~:text=More%20than%2080%20percent%20of,and%20production%20across%20the%20nation (accessed May 11, 2022).
6. Kim and Bae, "Korean Policies of Cybersecurity and Data Resilience."
7. Timothy Martin, "South Korea Fends Off Chinese, Russian Cyberattacks, U.S. Researcher Says," *The Wall Street Journal*, June 5, 2018, https://www.wsj.com/articles/south-korea-fends-off-chinese-russian-cyberattacks-u-s-researcher-says-1528194642 (accessed May 12, 2022).
8. The White House, "Fact Sheet: United States–Republic of Korea Partnership," May 21, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/21/fact-sheet-united-states-republic-of-korea-partnership/ (accessed May 11, 2022).
9. Kim and Bae, "Korean Policies of Cybersecurity and Data Resilience."
10. Yang Sung-jin, "Ransomware Attacks on Korean Companies on the Rise: KISA," *The Korea Herald*, August 2, 2021, http://www.koreaherald.com/view.php?ud=20210802000863 (accessed May 11, 2022).
11. Christopher Wray, "Director's Remarks to the Domestic Security Alliance Council," Federal Bureau of Investigation, April 27, 2022, https://www.fbi.gov/news/speeches/directors-remarks-to-the-domestic-security-alliance-council-042722 (accessed May 12, 2022).
12. News release, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," U.S. Department of Justice, February 17, 2022, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and (accessed May 11, 2022).
13. News release, "Justice Department Announces First Director of National Cryptocurrency Enforcement Team," U.S. Department of Justice, February 17, 2022, https://www.justice.gov/opa/pr/justice-department-announces-first-director-national-cryptocurrency-enforcement-team (accessed May 11, 2022).
14. James Rundle and Catherine Stupp, "Justice Department Installs New FBI Crypto Crime Unit," *The Wall Street Journal*, February 17, 2022, https://www.wsj.com/articles/justice-department-installs-new-fbi-crypto-crime-unit-11645129414 (accessed May 11, 2022).
15. Herb Scribner, "Treasury Sanctions Cryptocurrency Tool Tied to North Korean Hackers," Axios, May 6, 2022, https://www.axios.com/2022/05/06/treasury-cryptocurrency-tool-blender-north-korea (accessed May 11, 2022).
16. Jenna McLaughlin, "Estonia Hosts NATO-Led Cyber War Games, with One Eye on Russia," NPR, May 2, 2022, https://www.npr.org/2022/05/02/1095008257/estonia-nato-cyber-war-games-russia (accessed May 11, 2022).
17. Charlie Campbell, "South Korea's Intelligence Agency Has Joined NATO's Cyber Defense Unit. China Isn't Happy," *Time*, May 5, 2022, https://time.com/6173812/south-korea-cyber-nato-china/ (accessed May 11, 2022).
18. Hu Xijin, "If South Korea takes a path of turning hostile against its neighbors, the end of this path could be a Ukraine," Twitter post, May 4, 2022, 11:55 p.m., https://twitter.com/HuXijin_GT/status/1522062382666682369 (accessed May 11, 2022).
19. Avril Haines, "Annual Threat Assessment of the U.S. Intelligence Community, Opening Statement," U.S. Senate Armed Services Committee, May 10, 2022, https://www.dni.gov/index.php/newsroom/congressional-testimonies/congressional-testimonies-2022/item/2295-2022-ata-dni-opening-statement-as-delivered-to-the-sasc (accessed May 12, 2022).
20. Eurojust: European Union Agency for Criminal Justice Cooperation, https://www.eurojust.europa.eu/ (accessed May 19, 2022).
21. Rundle and Stupp, "Justice Department Installs New FBI Crypto Crime Unit."
22. Peter St. Onge, "A Revolution, If We Can Keep It: How Anti-NFT Regulations Threaten Financial Rights," Heritage Foundation *Issue Brief* No. 5256, March 22, 2022, https://www.heritage.org/government-regulation/report/revolution-if-we-can-keep-it-how-anti-nft-regulations-threaten.
23. Bruce Klingner, "North Korean Cyberattacks: A Dangerous and Evolving Threat," Heritage Foundation *Special Report* No. 247, September 2, 2021, https://www.heritage.org/asia/report/north-korean-cyberattacks-dangerous-and-evolving-threat.
24. Mark Pomerleau, "Why DoD Is Starting a New Cyber Cell on the Korean Peninsula," C4ISRNET, April 20, 2018, https://www.c4isrnet.com/dod/cybercom/2018/04/20/why-dod-is-starting-a-new-cyber-cell-on-the-korean-peninsula/ (accessed May 11, 2022).

25. Dustin Carmack, "U.S. Must Implement Lessons on 'Hybrid' Conflict from Ukraine War," Heritage Foundation *Backgrounder* No. 3704, April 28, 2022, https://www.heritage.org/cybersecurity/report/us-must-implement-lessons-hybrid-conflict-ukraine-war.
26. General Paul M. Nakasone, Commander, United States Cyberspace Command, testimony before the Committee on Armed Services, U.S. Senate, April 5, 2022, https://www.armed-services.senate.gov/hearings/-to-receive-testimony-on-the-posture-of-united-states-special-operations-command-and-united-states-cyber-command-in-review-of-the-defense-authorization-request-for-fiscal-year-2023-and-the-future-years-defense-program (accessed May 19, 2022).
27. News release, "United States Signs Protocol to Strengthen International Law Enforcement Cooperation to Combat Cybercrime," U.S. Department of Justice, May 12, 2022, https://www.justice.gov/opa/pr/united-states-signs-protocol-strengthen-international-law-enforcement-cooperation-combat (accessed May 12, 2022), and Martin Matishak, "Digital Cooperation by US, Ukraine Is a Success on Multiple Levels, Pentagon Chief Says," *The Record*, May 11, 2022, https://therecord.media/lloyd-austin-pentagon-us-ukraine-cyber-cooperation/ (accessed May 11, 2022)
28. The White House, "Fact Sheet: Quad Leaders' Summit," September 24, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/fact-sheet-quad-leaders-summit/ (accessed May 11, 2022).
29. Jeff M. Smith, "An Agenda for the 2021 Quad Summit: Five Next Steps," Heritage Foundation *Issue Brief* No. 5219, https://www.heritage.org/asia/report/agenda-the-2021-quad-summit-five-next-steps (accessed September 23, 2021).
30. Jeff M. Smith, "The Quad 2.0: A Foundation for a Free and Open Indo–Pacific," Heritage Foundation *Backgrounder* No. 3481, July 6, 2020, https://www.heritage.org/global-politics/report/the-quad-20-foundation-free-and-open-indo-pacific, and Klingner and Smith, "President Biden Should Strengthen Alliances During Asia Trip."
31. Kim and Bae, "Korean Policies of Cybersecurity and Data Resilience."
32. Carmack, "U.S. Must Implement Lessons on 'Hybrid' Conflict from Ukraine War."
33. The NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/ (accessed May 18, 2022).
34. Chris Riotta, "CISA's Public–Private Cyber Defense Group Helped Log4j Mitigation, Experts Say," *Federal Computer Week*, February 9, 2022, https://fcw.com/security/2022/02/cisas-public-private-cyber-defense-group-helped-speed-log4j-mitigation-experts-say/361793/ (accessed May 11, 2022).
35. Carmack, "U.S. Must Implement Lessons on 'Hybrid' Conflict from Ukraine War."
36. Australian Government, "Australia and the Republic of Korea Sign New MoU on Cyber and Critical Technology Cooperation," September 14, 2021, https://www.internationalcybertech.gov.au/Australia-and-Korea-sign-MoU (accessed May 11, 2022).
37. Ricky Ben-David, "Israel, South Korea Launch New Program for Robotics Tech Cooperation," *The Times of Israel*, April 14, 2022, https://www.timesofisrael.com/israel-south-korea-launch-new-program-for-robotics-tech-cooperation/ (accessed May 11, 2022).
38. U.S. Department of State, "Joint Statement on the U.S.–Japan–Republic of Korea Trilateral Ministerial Meeting," February 12, 2022, https://www.state.gov/joint-statement-on-the-u-s-japan-republic-of-korea-trilateral-ministerial-meeting/ (accessed May 11, 2022).
39. News release, "The 2nd ROK–UK Cyber Dialogue Held," South Korean Ministry of Foreign Affairs, January 29, 2020, https://www.mofa.go.kr/eng/brd/m_5676/view.do?seq=320935&srchFr=&srchTo=&srchWord=&srchTp=&multi_itm_seq=0&itm_seq_1=0&itm_seq_2=0&company_cd=&company_nm=&page=1&titleNm (accessed May 11, 2022).
40. David Inserra, "Cybersecurity Beyond U.S. Borders: Engaging Allies and Deterring Aggressors in Cyberspace," Heritage Foundation *Backgrounder* No. 3223, https://www.heritage.org/cybersecurity/report/cybersecurity-beyond-us-borders-engaging-allies-and-deterring-aggressors.
41. Catherine Stupp, "Updated Cybercrime Pact Aims to Speed Cross-Border Investigations," *The Wall Street Journal*, October 25, 2021, https://www.wsj.com/articles/updated-cybercrime-pact-aims-to-speed-cross-border-investigations-11635154202 (accessed May 11, 2022).
42. News release, "United States Signs Protocol to Strengthen International Law Enforcement Cooperation to Combat Cybercrime."