Quantum Leap: Improving Cybersecurity for the Next Era of Computing By Focusing on Users

Major W. Stone Holden
Michael Gerardi

ABSTRACT

The need to secure communications is critical for militaries and has offered an advantage in battle across history for those who do it well. The advent of new technologies offers ways of securing information, which appears impenetrable by the standards of their era, and this is true today. Quantum computing seems to provide a variety of benefits in defense applications, including protecting communications and the ability to decrypt information protected by some of today's encryption standards. While it is tempting to focus on investing heavily in quantum communications with the promise that this technology offers in securing communications, it would be foolish to ignore the human elements. This article brings historical parallels that offer insights into the potential weaknesses of heavy investment and application of this technology. Historical examples (specifically the experience of the Germans in World War II with their Enigma encryption machines) show that even the most capable encryption systems can be made ineffective by human error or laziness. Any investment by the defense community into quantum communications must be matched by an equal focus on developing a workforce that is more capable of properly handling and managing those systems, or the investment may be in vain. That investment should include improved cybersecurity training across the workforce and increased focus on Cybersecurity at Professional Military Education waypoints for

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

Maj W. Stone Holden is a Marine Officer assigned to Marine Aircraft Group 29, supporting the staff and subordinate helicopter squadrons in identifying and responding to emerging threats to operations. Previous assignments include the United States Southern Command, where he held billets in security cooperation and collections management, providing the opportunity to manage various projects implementing cutting-edge technological solutions to a range of threats in the AOR. He also served in the INDOPACOM AOR with 3rd Marine Regiment and Combat Logistics Battalion 3, deploying in support of the PACOM Augmentation Team Philippines (PAT-PHL) and aboard the USNS SACAGAWEA as part of Task Force KOA MOANA 17.

leaders. With these steps, the Department of Defense (DoD) may be able to avoid the mistakes of previous generations who relied too much on the promises of technology without shoring up the fragile humans who were essential to making that technology ultimately successful.

INTRODUCTION

The advantage in warfare often lies with those leaders who can communicate plans and messages to their forces rapidly, consistently, and securely. A further advantage lies with those who can penetrate, disrupt, or manipulate the communications of their adversaries. This is particularly true in the modern era of great power competition, where major international players have the resources and technological savvy to reasonably attempt to do both. Interestingly, emerging technologies hold the potential to secure communications in ways that are impenetrable by today's standards. Conversely, these same technologies can potentially render current encryption used by individuals and organizations around the world completely transparent. The driver behind this potential communications revolution is the promise of quantum computing and communications incorporating the unique properties of quantum physics. This technology has attracted the attention of many governments due to the potential benefits of securing their communications, the dangers of having their data decrypted by adversarial quantum computers, and the potential to do the same to their adversaries.[1] Although several years away from being a feasible technology to impact national security efforts, it is time to begin preparing for its arrival. A close examination of military history shows that relying on technical advances alone to secure communications is foolish. However, tomorrow's U.S. defense sector can avoid past mistakes by accounting for the human element in communications security.

Michael Gerardi is a Team Lead at Control Risks ONE Global Risk and Operations Centre (Americas). Michael manages and supports Senior Risk Consultants to ensure the identification, coordination, and response to real-time and future client risks. Prior to joining Control Risks, Michael served in the U.S. Marine Corps as an intelligence officer. Michael held various roles throughout his tenure, leading teams specializing in tactical aviation intelligence, strategic open source, and crisis intelligence. In 2021, Michael decided to transition from the Marines and further his education by pursuing a master's degree in science and international security from King's College London.

The U.S. Defense Science Board identified three areas of quantum technology that hold particular interest for the Department of Defense (DoD): quantum communications, quantum computing, and quantum sensing.[2] Of particular interest is the arrival of quantum communications and encryption, offering offensive and defensive implications for future communications security. The U.S. is leaping ahead to research and develop quantum technologies, doubling the government investment between 2019 and 2021 and hovering at nearly $1 billion annually since then.[3] As with any new technology, there is a risk of focusing too much on the technology itself and ignoring the users who will ultimately implement or use it. It is critical to pair future communications and cyber systems with improved training and education of personnel. While quantum communications offer a more secure means to pass information, and quantum computing provides the potential for leaps in encryption and decryption capabilities, human factors remain a constant threat to even the most secure technology.

DISCUSSION

The advances offered by quantum technologies have historical analogs that can provide insight into how they may impact national security. Militaries have been trying to intercept and decode the communications of their rivals since antiquity. Encryption is one common way to protect information. It is the process of transforming a form of otherwise readable data (or "plaintext") into a form that obscures the original meaning of the data (or "ciphertext") to prevent it from being known or used without a special piece of information (or "key") which can be applied to turn the data back into a readable form.[4] In antiquity, the Spartans invented a device for message encryption called a scytale, which may have been used to obscure the meaning of communications from adversaries.[5] Efforts to encrypt information more securely contin-

ued in states around the world, with various societies developing manual cryptographic means of securing communications up to the dawn of the industrial age.[6] WWII saw the application of industrial organization and machinery to the task of protecting and acquiring communications. Today's encryption methods vary in technique and strength of protection but generally break into asymmetric and symmetric encryption. Asymmetric encryption (commonly referred to as public key cryptography) is a method that uses two separate keys to exchange data, with one encrypting the data and one decrypting the data.[7] The alternative is symmetric cryptography, which uses the same secret key for encrypting the data being sent and for reversing that encryption by the receiver).[8] The information advantage gained by breaking into the secure communications of an opponent can provide militaries with a defining factor in the success or failure of achieving its objectives.[9] It is critical, therefore, that the U.S. continues the task of breaking encrypted communications while fiercely protecting its own against capable adversaries. This requires the adoption and employment of innovations, including quantum technology, in defense of U.S. information and communications and an offensive means to intercept and understand the communications of adversaries. With the re-emergence of Great Power competition, the need for secure communications is increasingly pressing.[10,11]

Currently, secure military communications employ a series of countermeasures to ensure they are not intercepted or read by others. Frequency hopping is one method, referring to wireless communications that rapidly and randomly change the frequency they are transmitting and receiving to avoid interception.[12] A portion of a message may be intercepted, but not enough to be useful. Encryption, another method for securing communications, scrambles a message in a way that makes it mathematically improbable that an adversary could unscramble the message in a reasonable or helpful amount of time without the "key" for decrypting it.[13] Both of these methodologies are commercially available and employed by U.S. forces but remain challenging for most militaries to implement.

Russian forces have been notorious for communicating "in the clear" during their invasion of Ukraine in 2022. Their failure to use encryption or frequency hopping for their military communications has left the world with access to snippets of some of the most intimate battlefield communications. Failure to use existing communications security measures stems from a lack of capable systems in the Russian military at the operational and tactical levels and a failure of training on how to employ them properly. These security failures allowed Ukrainian forces to intercept and act on Russian radio communications.[14] At the same time, foreign observers gained insights into Russian tactics and operational struggles.[15] Communications security based on state-of-the-art technological methodologies means little when personnel employing them are incapable of doing so or are unwilling to do so correctly.

Quantum technologies have defensive, zero-trust implications for communications security through quantum key distribution (QKD).[16]

> In QKD, an encryption key is transmitted between the two communicating parties in the form of quantum particles called photons. As a result of the quantum nature of these particles, any eavesdropper who intercepts them will, in principle, necessarily leave a signature on the data stream itself; if the protocol is implemented properly, then it is physically impossible to observe the photons without modifying them in a way.[17]

QKD is currently a difficult task, limited by the need for a quantum channel to allow the exchange of photons and restricted by distance for quantum channels built using existing ground-based fiber optic technology,[18] but it provides an interesting alternative that is attractive to many working in industries or agencies requiring secure communications.

Quantum computing also offers a tool with more offensive uses. Standard computers today use "bits" of information composed of a string of binary characters that can either be "1" or "0." Quantum computers harness properties of quantum physics to store and transmit information in "qubits." Instead of reducing information to binary forms, qubits have four different possible positions at any given time. This allows quantum computers to rapidly run special algorithms and perform select functions that take standard computers thousands of years in a matter of days or hours.[19] This could lead to a shift from hackers trying to bypass cryptologic systems to hackers leveraging quantum capabilities to attack the system itself.[20] While current encryption methods employed by the government and military are secure, the potential for hackers to attack the system rather than merely bypass it is still concerning and will need to be addressed. Quantum key distribution and quantum computing represent extraordinary technological advances that have the potential for significant impacts on communications security.

Even amid what may seem like unprecedented times, there are significant echoes of a previous era of Great Power competition and communications security. In WWI, the rise of radio-based wireless communication significantly increased communication speed, but serious security flaws were associated with its use. Skilled radio operators could intercept these communications, using positional data to find transmitters and either read messages in the clear or manually decrypt them. The Germans suffered for their insecure communications in the naval battles of the Pacific, where their losses could at least be partially placed at the feet of insecure communications.[21] This was an example of poor technical security, with operators transmitting in ways that could be intercepted due to a lack of technological capability to encrypt or protect that information adequately. Furthermore, it also demonstrates the human failures of the operators, who were not taking appropriate steps to obscure communications using simple tools available in that era.

In the years leading up to WWII, technological innovations in electrical communication and mechanical engineering allowed the Axis powers to improve their communications technology, taking advantage of the increased speed and security.[22] At the start of WWII, the Germans made a concerted effort to adopt a range of emerging technologies to improve

their communications. The incorporation of radio, the Enigma machine to secure messages with front-line troops, and the even more secure and faster Lorenz machine for high-level messages all drastically changed the pace and security of their communications.[23,24] German capitalization on the speed offered by electronic communications tools, including Enigma, was pivotal in their early Blitzkrieg campaigns. It allowed them to coordinate the masses of troops enabled by industrialization across a large front while maintaining a blistering pace of warfare.[25] While keen to seize the technological edge, the Germans were also highly security conscious and became early adopters of modern communications security protocols and encryption methods.[26]

As part of their security efforts, the Germans adopted the Enigma code machine for employment in military operations.[27] When used properly, the Enigma offered 150 quintillion distinct ways to set it up to encode a message. In an age before modern computers, this should have rendered it practically unbreakable to anyone trying to snoop.[28,29] The machine was revolutionary and created tremendous difficulty for the Allied war effort since code-breaking consumed enormous amounts of British and American resources. Breaking the code eventually occurred with the help of some of the most brilliant minds of the time from Poland, the United Kingdom, and the U.S[30] Successful harnessing of the intellectual capital of their nations was a pivotal element to Allied success. However, more was needed to beat the Enigma system.

A major contributing factor in breaking the Enigma code was consistent human error by well-trained and highly skilled German Enigma operators.[31] Simple mistakes (like failing to completely switch out the coded wheels that adjusted the encryption, typing repetitive messages, and encoding messages in both old and new settings) proved critical shortcomings that allowed Allied cryptanalysts to ultimately penetrate Enigma. The technological promise of completely secure communications had lured operators into a false sense of security. If no one could break this code, why put so much effort into the surrounding security protocols and practices? The human factor of the operators succumbing to natural tendencies to take shortcuts while underestimating the impact of failure to adhere to established protocols. All these factors are amplified in times of conflict, when extreme fatigue, stress, and grueling mental workloads wear away at the finer elements of human precision.[32] Sometimes, it makes little sense to spend time breaking codes when you can bypass them altogether through the system's weakest link.

Contrasting the painstaking labor by the Allies to break Axis codes, Italian agents relied on the laziness of physical security protocols at Allied embassies to acquire cipher books and decrypted communications.[33] Terrible security protocols in vetting employees allowed Italian agents to penetrate U.S. embassies and gain access to office spaces after hours. Once inside, the embassy security protocols (when followed) were ridiculously simple to overcome. Keys were unsecured, documents were left out in the open, and safes required no more

than a screwdriver to remove a back panel. These relaxed security procedures all went to aid Italian agents. The best encryption methods in the world could be easily bypassed by exploiting human laziness and error. In this instance, those tendencies provided a wealth of information to Axis forces. German leaders like Field Marshall Erwin Rommel were able to conduct their early campaigns with a wealth of information that it was like "... a gambler, but one who could read the other player's cards."[34] These types of errors are not a thing that we can toss into the dustbin of history, as something that was solely a flaw of another generation.

Just as Germany capitalized on emerging advances in information security presented by mechanical encryption, the U.S. is investing in its emerging technologies. The U.S. has completed a significant amount of work to prepare for quantum technologies on the technical side of the issue. Since 2019, the U.S. government has spent over $2.5B on quantum research and development.[35] This investment resulted in notable achievements, including the announcement in July 2022 by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) that it had selected some of the first tools designed specifically to withstand quantum decryption.[36] This is a major technical step toward communications security in the post-quantum world, but more is needed.

In the decades following the Cold War, the U.S. has primarily fought against non-state adversaries who have not enjoyed the sophisticated communications capabilities states can field. This has led to a sense of invulnerability, which contributed to embarrassing communications security failures- like when Iraqi insurgents hacked military unmanned aerial system data feeds.[37] It is tempting to believe that our military forces and populations, in general, have evolved from the kind of human error that proved fatal to the brilliance of the Enigma in WWII. It would be unwise to do so. The threats posed to secure military communications continue to be substantial and will likely be exacerbated by technological advances. The People's Republic of China (PRC) has listed quantum computing as one of the technologies they are pursuing to seize the "technological high ground." The contemporary battlefield is already seeing the application of advanced technology that will significantly impact communications in modern warfare.[38,39] The advances in quantum communications and quantum key distribution offer the allure of making communications so secure that they are practically unbreakable with the current technology.[40,41] These advances can also work against the U.S.

It is plausible that soon, aggressors will be able to use quantum computing tools to attack U.S. communications in novel ways while also using technology like quantum computing to fortify their communications against U.S. penetration.[42] Technology is not the only solution; its advantage is often fleeting and rarely as dominant as first perceived.[43] Any pursuit of a technological solution to the problem of employing quantum technologies to protect U.S. data or to defeat adversary communications security needs to incorporate the human design element of cybersecurity. The most advanced technologies in the hands of someone who mishandles it can be undermined by their actions.

Human error remains a significant attack surface for communications penetration. Every year, millions of dollars are invested worldwide in sophisticated cyberattacks, painstakingly built off of millions of lines of precise coding. Many of these attacks rely on human error to gain their fatal foothold. Spearfishing, failing to update systems, and weak passwords contribute to a substantial number of successful attacks.[44,45] A 2014 study by IBM found that across 130 countries, over 95 percent of all cybersecurity incidents could be traced back to human error at some point.[46] The report showed that these errors included misconfiguration of systems (like with the Enigma wheels), poor patch management (similar to German operators failing to update their codes), bad passwords, and poor control of devices (reminiscent of the poor embassy security exploited by the Italians). A 2022 white paper by Mandiant discussed human error's impact on a cyberattacks success. It noted that poor training of employees contributed to their seeming inability to stop making security mistakes that left their organizations open to penetration.[47] Any system that emerges based on quantum computing must be designed to guard against human errors that can render it vulnerable on either end of the communications link.

Communications protected by quantum technologies are more resistant to interception attempts and decryption, but must still be transferred onto a computer for the end user to consume. This remains vulnerable to hacking or attacks that could reveal the "secured" information.[48] Securing the technical middle, without securing the human operators on either end, ignores the broadest surface for communications penetration. Human error remains a primary contributing factor to the penetration of communications security protocols in the cyber domain, and there is little evidence to suggest that the trend will change.

Despite large amounts of time and resources applied to cybersecurity, DoD currently struggles to maintain cybersecurity across one of the largest workforces of any organization on the planet.[49,50] The Federal government spends over $100 billion annually on cyber and information technology investments.[51] Even with this level of investment, in 2019, the Government Accountability Office revealed over 28,000 reported cybersecurity incidents.[52] While not every incident will be the critical error that unleashes the adversaries waiting in the shadows, the sheer scale of the problem increases the risk it poses to DoD. The DoD is massive, with millions of personnel needing to access systems at different levels and for other purposes.[53] Furthermore, diverse backgrounds and educational experiences make it difficult to adopt and implement sweeping policies effectively. An officer falls for a spearfishing attack; a soldier or sailor leaves their credentials somewhere by accident; a janitor at a facility finds a thumb drive and pops it into a machine to see who owns it; a tired field operator fails to properly execute all of the security protocols for their communications device. These problems will not abate with the emergence of quantum computing.

Current levels of cybersecurity training for DoD members fall well short of where they should be despite its prominence in strategic guidance documents. The 2018 DoD Cyber Strategy lists four objectives. Two of those, defending U.S. critical infrastructure from cyberattacks and

protecting DoD information and systems from cyber threats, demand a greater level of training and education in the general user population.[54] The strategy also identifies the importance of cultivating a more robust cybersecurity culture within the larger workforce and the value of providing training for personnel on cyber topics.[55] In cultivating this cyber-proficient workforce, more effort should be expended on raising the general level of cyber awareness among non-IT professionals. These personnel play a critical role in maintaining the security of information systems.

The annual DoD-mandated cybersecurity training provides little more than a baseline of "what not to do." Improved training should discuss actual threat actors and real compromises and provide tactics, techniques, and procedures for adversaries. Better training would provide users with case studies highlighting why training is so relevant and how adversaries seek to undermine their security. Building upon the foundation of the annual cyber awareness training allows training to progress to more complicated and nuanced issues. Training must also be supplemented with more general education on cyber topics as DoD members progress in their careers. While some courses on cyber topics are available at the Naval Postgraduate School, Army War College, and Air Force Institute of Technology, there is room for improvement.[56,57] Updated rigorous cyber course requirements at each Professional Military Education checkpoint throughout a career are an easy way to improve the cyber-savvy of leaders across the joint force.[58] A mix of improved training and better education of leaders would go a long way toward addressing the human side of information security risks. Nurturing a cyber security-oriented joint force will pave the way to reduced risks associated with implementing quantum communications systems within DoD.

CONCLUSION

While investing in cutting-edge technology is important, the U.S. must apply historical lessons about human vulnerability to its future communications security efforts. People are capable of amazing things, but innate traits are also often the weak link in the chain of communications security. Though failure and accidents will always be a part of technological systems, they must be designed to minimize the chance of error, dull the allure of laziness, and anticipate the friction of war, which could lead to security-compromising behaviors. By embracing the hard-won lessons of WWII and evolving them to apply to the advances of the modern era, the U.S. national security enterprise and DoD can position itself on the road to success in the communications security battles of the future.

DISCLAIMER

The views and opinions expressed herein are those of the authors, alone, and do not necessarily reflect the official policy or position of the United States Marine Corps, the Department of Defense, the U.S. Intelligence Community, or the U.S. Government.

NOTES

1. Michael J. D. Vermeer and Evan D. Peet, "Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption," Santa Monica, CA: RAND Corporation, 2020, https://www.rand.org/pubs/research_reports/RR3102.html, 1.
2. Congressional Research Service, "Defense Primer: Quantum Technology," *In Focus*, September 2022, https://crsreports.congress.gov/product/pdf/IF/IF11836, 1.
3. Subcommittee on Quantum Information Science Committee on Science, "NATIONAL QUANTUM INITIATIVE SUPPLEMENT TO THE PRESIDENT'S FY 2023 BUDGET," National Science and Technology Council, January 2023, https://www.quantum.gov/wp-content/uploads/2023/01/NQI-Annual-Report-FY2023.pdf.
4. National Institute of Standards and Technology, "Encryption," Computer Security Resource Center, accessed 9 Mar 2024, https://csrc.nist.gov/glossary/term/encryption.
5. Martine Diepenbroek, "The Spartan Scytale," https://www.academia.edu/download/65378844/ Diepenbroek.pdf, 46-47.
6. Gustavus J. Simmons, "Cryptology," *Encyclopedia Britannica,* https://www.britannica.com/topic/ cryptology/History-of-cryptology.
7. National Institute for Standards and Technology, "Asymmetric Cryptography," Computer Security Resource Center, accessed March 9,, 2024, https://csrc.nist.gov/glossary/term/asymmetric_cryptography.
8. National Institute for Standards and Technology, "Symmetric Cryptography," Computer Security Resource Center, accessed March 9, 2024, https://csrc.nist.gov/glossary/term/symmetric_cryptography.
9. Jack Detsch and Amy Mackinnon, "'The Ukrainians Are Listening': Russia's Military Radios Are Getting Owned," *Foreign Policy,* 2022, https://foreignpolicy.com/2022/03/22/ukraine-russia-military-radio/.
10. CSIS, "Reversing the Tide: Toward a new U.S. strategy to support democracy and counter authoritarianism," Task Force on US Strategy to Support Democracy and Counter Authoritarianism, April 2021, 5-7, 25-26.
11. US Office of The Director of National Intelligence, 2021 Annual Threat Assessment of the U.S. Intelligence Community, 2021, 5-11.
12. United States Marine Corps, "Communication Equipment B191716 Student Handout," https://www.trngcmd.marines.mil/Portals/207/Docs/TBS/B191716%20Communication%20Equipment.pdf, 11-12.
13. Vivek Wadhwa and Mauritz Kop, "Why Quantum Computing Is Even More Dangerous Than Artificial Intelligence," *Foreign Policy,* August 2022, https://foreignpolicy.com/2022/08/21/quantum-computing-artificial-intelligence-ai-technology-regulation/.
14. Detsch and Mackinnon, "The Ukrainians."
15. *The Economist*, "Why Russian radios in Ukraine are getting spammed with heavy metal," May 2022, https://www.economist.com/the-economist-explains/2022/03/28/why-russian-radios-ukraine-war-intercepted-heavy-metal.
16. Edward Parker, "Commercial and Military Applications and Timelines for Quantum Technology," Santa Monica, CA: RAND Corporation, 2021, https://www.rand.org/content/dam/rand/pubs/research_reports/ RRA1400/RRA1482-4/RAND_RRA1482-4.pdf, 8-9.
17. Parker, "Commercial and Military Applications and Timelines for Quantum Technology," 18
18. Bruno Huttner, Romain Alleaume, et al., "Long-range QKD without trusted nodes is not possible with current technology," npj *Quantum Information* 8, 108 (2022), https://doi.org/10.1038/s41534-022-00613-4.
19. Michael J. D. Vermeer and Evan D. Peet, "Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption," Santa Monica, CA: RAND Corporation, 2020, https://www.rand.org/pubs/research_reports/RR3102.html, 5.
20. Vermeer and Peet, 5-6.
21. John Keegan, *Intelligence in War: Knowledge of the Enemy From Napoleon to Al-Qaeda*, (New York: Random House, 2003), 105-143.
22. Alex Hern, "How did the Enigma machine work?" The Guardian, November 2014, https://www.theguardian.com/technology/2014/nov/14/how-did-enigma-machine-work-imitation-game.
23. The History Press, "How Lorenz was different from Enigma," accessed May 8, 2023, https://www.thehistorypress.co.uk/articles/how-lorenz-was-different-from-enigma/.

NOTES

24. Stanford University, "The Lorenz Schluesselzusatz SZ40/42," accessed May 9, 2023, https://cs.stanford.edu/people/eroberts/courses/soco/projects/2008-09/colossus/lorenzmachine.html.
25. Max Boot, *War Made New: Weapons, Warriors, and the Making of the Modern World,* (New York: Penguin Group Publishing, 2006), 223-236.
26. Max Hastings, *The Secret War: Spies, Ciphers, and Guerillas 1939-1945,* (New York: HarperCollins Publishers, 2016), 7-8.
27. Gershom Gorenberg, *War of Shadows: Codebreakers, Spies, and the Secret Struggle to Drive the Nazis from the Middle East*," (New York: Public Affairs, 2021), 63-70.
28. Gorenberg, 67.
29. Mark Lowenthal and Robert Clark, *The 5 Disciplines of Intelligence Collection*, (Thousand Oaks, CA: Sage Publishing, 2016), 90-95.
30. Gorenberg, 81-92.
31. Gorenberg, 88-92.
32. CL Paul and J Dykstra, "Understanding Operator Fatigue, Frustration, and Cognitive Workload in Tactical Cybersecurity Operations." *Journal of Information Warfare* 16, no. 2 (2017), https://www.jstor.org/ stable/26502752, 2-4.
33. Gorenberg, 349-361.
34. Gorenberg, 311.
35. Subcommittee on Quantum Information Science, "NATIONAL QUANTUM INITIATIVE SUPPLEMENT TO THE PRESIDENT'S FY 2022 BUDGET," National Science and Technology Council, December 2021, https://www.quantum.gov/wp-content/uploads/2021/12/NQI-Annual-Report-FY2022.pdf, 6-8.
36. NIST.gov, "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," July 2022, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.
37. Mike Mount and Elaine Quijano, "Iraqi insurgents hacked Predator drone feeds, U.S. official indicates," CNN, December 2009, http://www.cnn.com/2009/US/12/17/drone.video.hacked/index.html.
38. US Army Training and Doctrine Command, "The Operational Environment and the Changing Character of Future Warfare," 2018, 14.
39. Rush Doshi, *LONG GAME: China's Grand Strategy and the Displacement of American Power,* (Oxford University Press, 2021), 263-265, 286.
40. US Congressional Research Service, "Defense Primer: Quantum Technology," Report IF11836, version 5, December 2021, 2.
41. Edward Parker, "Commercial and Military Application and Timelines for Quantum Technology, RAND Corporation, 2021, 8-10, 14-16.
42. Center for Strategic and International Studies, "Maintaining The Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation," CSIS Technology and Intelligence Task Force, January 2021, 5.
43. Ian Sullivan "300. "Once More unto The Breach Dear Friends": From English Longbows to Azerbaijani Drones, Army Modernization STILL Means More than Materiel," https://madsciblog.tradoc.army.mil/300-once-more-unto-the-breach-dear-friends-from-english-longbows-to-azerbaijani-drones-army-modernization-still-means-more-than-materiel/.
44. Nicole Perlroth, "This Is How They Tell Me the World Ends: The Cyberweapons Arms Race," (New York: Bloomsbury Publishing, 2021), 337, 341, 397.
45. Kaspersky, "The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within," Kaspersky Daily, Kaspersky.com, 2017.
46. IBM Global Technology Services, "IBM Security Services 2014 Cyber Security Intelligence Index," Managed Security Services, 2014, https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom /IBMSecurityServices2014.PDF, 1-4.
47. Mandiant, "Navigating the Cyber Skills Shortage," June 2022, https://www.mandiant.com/sites/default/files/2022-06/navigating-the-cyber-skills-shortage-wp.pdf.
48. Edward Parker, "Commercial and Military Applications and Timelines for Quantum Technology," RAND, https://www.rand.org/content/dam/rand/pubs/research_reports/RRA1400/RRA1482-4/RAND_RRA1482-4.pdf, 2021, 8-9.

NOTES

49. Henry Taylor, "Who is the world's biggest employer? The answer might not be what you expect," The World Economic Forum, Jun 2015, https://www.weforum.org/agenda/2015/06/worlds-10-biggest-employers/#:~:text=It's%20often%20said%20that%20Indian,million%20employees%20on%20its%20roster.
50. Martin Armstrong, "The World's Biggest Employers," Statista, November 2022, https://www.statista.com/chart/3585/the-worlds-biggest-employers/.
51. Government Accountability Office, "Information Technology and Cybersecurity: Using Scorecards to Monitor Agencies' Implementation of Statutory Requirements," GAO.gov, July 2022, https://www.gao.gov/products/gao-22-106105.
52. Government Accountability Office, Cybersecurity," GAO.gov, accessed October 10, 2022, https://www.gao.gov/ cybersecurity.
53. US Government Accountability Office, "CYBERSECURITY: DoD Needs to Take Decisive Actions to Improve Cyber Hygiene," Report to Congressional Committees, April 2020, https://www.gao.gov/assets/gao-20-241.pdf, 1-4.
54. Department of Defense, "Summary: Department of Defense Cyber Strategy," 2018, 3.
55. Department of Defense, "Summary: Department of Defense Cyber Strategy," 2018, 6.
56. US Army War College, "Curriculum," https://ssl.armywarcollege.edu/dde/curriculum.cfm, accessed 12 October 12, 2022.
57. Naval Postgraduate School, "Cyber Security and Operations Courses," https://nps.edu/web/c3o/course-list, accessed October 12, 2022.
58. Erica Borghard, Mark Montgomery, and Brandon Valeriano, "The Challenge of Educating the Military on Cyber Strategy," *War on the Rocks*, June 2021, https://warontherocks.com/2021/06/the-challenge-of-educating-the-military-on-cyber-strategy/.