Security Analysis, 2021-2024:
Understanding Which Threats to Watch

Rachael Riggs

Henley-Putnam School of Strategic Security

National American University

INT511 Advanced Analytical Methods

Amie Bowman

December 2020

Security Analysis, 2021-2024:
Understanding Which Threats to Watch

Key Judgements

Technology is advancing at paramount speeds, and keeping up with this security has proven to exacerbate. Knowing which threats can cause the most damage and which threat actors we need to watch for is essential to aim our focus.

- The rapid growth of technology makes cyber-warfare[1] Our largest concern.
- Threats are substantial with Organized Criminal Organizations, and one should not ignore the severity. However, the most significant threat we face with cyber warfare is that with nation-states and nation-state funding to such criminal organizations.[2]
- Malicious use of AI, Disinformation campaigns, hacking, and ransomware are at the top of the list of threats we face in the U.S.
- Russia, China, North Korea, and Iran are the nation-states that are the biggest threats to America's security.
- Our best defense is the education and training of employees and government, corporate, academic, and scientific community collaboration.

Introduction

This report focuses on the current threats the United States faces. One of our country's most substantial threats involves advanced technology and the damage it can create. The analysis shows that while other actors remain a threat, America's most significant threat concerning

[1] Cyber Warfare is defined as the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attack of information systems for strategic or military purposes.

[2] For an extensive list of state-sponsored hacking events, visit the Center for Strategic and International Studies Website at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

technology belongs to nation-states, precisely that of Russia, China, North Korea, and Iran. (Homeland Threat Assessment, 2020)

Background

Deep fakes are a tool capable of swapping faces and voices in photos and video. Deep Fake technology, when used maliciously, can create massive chaos and destruction. Deep Fakes are created when a person uses a facial recognition algorithm and a deep learning computer network (Somers, 2020) to swap images, video, or audio with another person; this can happen for entertainment and many other reasons. However, when done maliciously, the damage would be large-scale. A leader giving a speech he never gave, a fake voice for voice recognition, or a company owner transferring money are just a few examples of how Deep Fakes could cause catastrophic consequences.

There are a few ways that a person can detect a Deep fake without software. A few ways to spot one include noticing that a person is blinking too much, their hairline is off, a pixilation difference, and if they are wearing glasses, check to see that the reflection matches the scene. (Somers, 2020) The sophistication of this technology can make it hard for the naked eye to spot.

Russia, China, North Korea, and Iran currently threaten America's national security. Summing up Russia's intentions in a September Signal Magazine article, "Russia has built a disinformation ecosystem that tries to promote anything that drives a wedge between the United States and our allies." (Ackerman, Russia Weaponizes Increasingly Sophisticated Disinformation, 2020) Ackerman goes on to state the five areas Russia has put their focus on:

- state-funded global messaging
- The cultivation of proxy sources

- official government communications
- weaponizing social media
- cyber-enabled disinformation. (Ackerman, Russia Weaponizes Increasingly Sophisticated Disinformation, 2020)

The DOJ's information on their China Initiative states that 80% of economic espionage prosecutions include conduct beneficial to China. It also states that 60% of all trade secret theft cases are somehow related to China. (The United States Department of Justice, 2020)

Russia and China are the most significant threats to the security of the United States, but Iran and North Korea pose a genuine cyber espionage threat. (Pompeo, 2020) (United States Institute of Peace, 2020) North Korea is advancing its already sophisticated nuclear weapons and missile program, which should be of significant concern in addition to cyber warfare threats. (Nikitin, 2020)

Substantiation

Technology advancements pose a significant threat to the United States. The most prominent cyber threat actors are nation-states. Technological refinements occur daily, and as we progress into a society that heavily relies on these advancements, we must understand the dangers we face as a nation. Disinformation campaigns[3], influence operations,[4] Moreover, the theft of government and corporate secrets threatens our national security and American democracy. (Zegart, 2020) Four nation-states harbor the most significant threat to the United States. Those four main threats include Russia, North Korea, China, and Iran. (Ackerman, 2020)

[3] Disinformation Campaigns are state-sponsored and use disinformation, which is false or misleading information, and spread the information to deceive, confuse, or cause significant problems.

[4] The Rand Corp defines influence operations as "the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent."

Technology improvements, in combination with disinformation operations, have the potential for catastrophic consequences. Artificial Intelligence[5] It brings with it such technology to create Deep Fakes and the ability to bypass physical recognition. (Hao & O'Neill, 2020) Bypassing facial recognition has shown to be highly detrimental, such as McAfee's testing of passport scans in an airport, which tricked the system into allowing a person through who is on the "do not fly" list. (Povolny, 2020) Deep Fake technology, if used strategically, could cause such undesirable results as mass confusion, riots, rebellion, revolt, nationwide distrust, and potentially much worse repercussions.

Hacking and Ransomware[6]Continue to grow on the threat scale. In addition to what we face with AI, we should remain concerned about hacking and ransomware, which continue to expand as a national security threat. Beyond the stealing of state secrets and technological blueprints, WMD should be of great concern. As we have seen with the Coronavirus pandemic, the threat of bioweapons is real.

America needs to focus correctly to stay on top of cyber issues. The U.S. has spent the past decade on counterterrorism, domestic issues, and the Coronavirus. We could have focused on technological advancements and more robust security with that time lost. We need to make that the focus now. (Sadat, 2020)

The four countries that have proven to be America's most substantial threat have their own objective and focus. Russia strives to obtain the spot of the world's superpower. The country focuses on AI used in disinformation operations, propaganda, surveillance, and military

[5] Artificial Intelligence: “the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages."

[6] Ransomware: malicious software that infects your computer and displays messages demanding a fee to be paid for your system to work again. It can lock a computer screen or encrypt important, predetermined files with a password.”

systems such as UAVs to attain this. (Sayler, 2020) China has focused on using A.I. for facial recognition and surveillance measures. China's interests are in counterespionage, surveillance, and military efforts. (Sayler, 2020) China has been America's most significant threat regarding hacking (Thompson, 2020) and theft of information (FBI.Gov, 2020); because of this, countermeasures need to be a strong focus, and American companies need to be involved in deterring these activities. North Korea has focused on strengthening its nuclear weapons and missile program. Iran and North Korea have used disinformation campaigns, undergone cyber espionage, and frequently support criminal cyber threat actions against the United States via state-sponsored activities. (Homeland Threat Assessment, 2020)

Context

This assessment focuses on one of the United States' most significant threats, technology, and the issues arising from technological advancements. Furthermore, it discusses which countries are the biggest threat to our National Security. The threats to America's national security encompass many areas, and new threat actors appear daily. However, knowing what is known now, we can narrow our focus to the four stated in this report. Technology has many aspects that provide great value, but it also opens the doors to new threats our country has yet to encounter. The best way to counter these threats is to be prepared for them, understand them, and realize the impact that each of these threats could impose on us.

Conclusion/Recommendation

Our best defense against these attacks is to stop them before they occur. Our best line of defense is working with tech companies to create new technology to help diminish the dangers involved, bringing in great minds to help create solutions, and hiring and training employees to spot and deter attacks.

Creating and maintaining a solid network of collaborators within government, academia, corporate, and the scientific community sectors is essential. Bringing these groups of people together frequently to work together and aid in protecting the nation will provide the most significant benefits. The Carnegie Endowment for International Peace stresses this need with their Research on Influence Operations. (Shapiro, Thompson, & Wanless, 2020)

Collaboration, but mostly employee education and training, must be stressed more of their importance. These recommendations will benefit our country's security. Mainly, A strong emphasis needs to be put on every company, ensuring that their employees understand threats, how they can happen, ways to avoid and mitigate threats, and to know when they are being targeted. Ensuring an employee has this knowledge is not only essential but absolutely critical.

T

References

Ackerman, R. K. (2020, August 28). China Heads List of International Technology Thieves. *Signal*, p. 1. Retrieved from https://www.afcea.org/content/china-heads-list-international-technology-thieves

Ackerman, R. K. (2020, September 4). Russia Weaponizes Increasingly Sophisticated Disinformation. *Signal*, p. 1. Retrieved from https://www.afcea.org/content/russia-weaponizes-increasingly-sophisticated-disinformation

FBI.Gov. (2020, November 16). *The China Threat*. Retrieved December 2020, from FBI.Gov: https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans

Hao, K., & O'Neill, P. H. (2020, August 5). The hack that could make face recognition think someone else is you. *MIT Technology Review*, p. 1. Retrieved from https://www.technologyreview.com/2020/08/05/1006008/ai-face-recognition-hack-misidentifies-person/

Homeland Threat Assessment. (2020). *Homeland Threat Assessment.* Department of Homeland Security. Washington DC: www.dhs.gov. Retrieved from https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf

Nikitin, M. B. (2020). *North Korea's Nuclear Weapons and Missile Programs.* CRS Report, Congressional Research Service, Washington DC. Retrieved from https://crsreports.congress.gov/product/pdf/IF/IF10472

Pompeo, M. R. (2020, September 17). *The United States Sanctions Cyber Actors Backed by Iranian Intelligence Ministry*. Retrieved from WWW.State.Gov:

https://www.state.gov/the-united-states-sanctions-cyber-actors-backed-by-iranian-intelligence-ministry/

Povolny, S. (2020, September 14). *How McAfee Researchers Successfully Bypassed Facial Recognition Verification Technology with A.I*. Retrieved from WWW.HomelandSecurityToday.US: https://www.hstoday.us/subject-matter-areas/airport-aviation-security/how-mcafee-researchers-successfully-bypassed-facial-recognition-verification-technology-with-ai/

Sadat, M. (2020, October 18). *America must build its technology industries to win against China and Russia*. Retrieved from The Hill (Opinion Contributor): https://thehill.com/opinion/technology/521088-america-must-build-its-technology-industries-to-win-against-china-and

Sayler, K. M. (2020). *Emerging Military Technologies: Background and Issues for Congress.* Washington D.C.: Congressional Research Service. Retrieved from https://fas.org/sgp/crs/natsec/R46458.pdf

Shapiro, J. N., Thompson, N., & Wanless, A. (2020, December 3). *Research Collaboration on Influence Operations Between Industry and Academia: A Way Forward*. Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/2020/12/03/research-collaboration-on-influence-operations-between-industry-and-academia-way-forward-pub-83332

Somers, M. (2020, July). Deepfakes, Explained. *MIT Management Sloan School*. Retrieved from https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained

The United States Department of Justice. (2020, November 12). *INFORMATION ABOUT THE DEPARTMENT OF JUSTICE'S INITIATIVE AND A COMPILATION OF CHINA-*

RELATED PROSECUTIONS SINCE 2018. Retrieved from Justice.Gov: https://www.justice.gov/opa/information-about-department-justice-s-china-initiative-and-compilation-china-related

Thompson, T. (2020, October 8). *How Congress Can End China's Theft of U.S. Military Secrets*. Retrieved from Real Clear Defense: https://www.realcleardefense.com/articles/2020/10/08/how_congress_can_end_chinas_theft_of_us_military_secrets_580027.html

United States Institute of Peace. (2020, October 13). *The Iran Primer*. Retrieved from United States Institute of Peace: https://iranprimer.usip.org/blog/2020/oct/13/four-iranian-threats-us-homeland

Zegart, A. (2020, November 2). *Intelligence Isn't Just for Government Anymore*. Retrieved from Foreign Affairs: https://www.foreignaffairs.com/articles/united-states/2020-11-02/intelligence-isnt-just-government-anymore