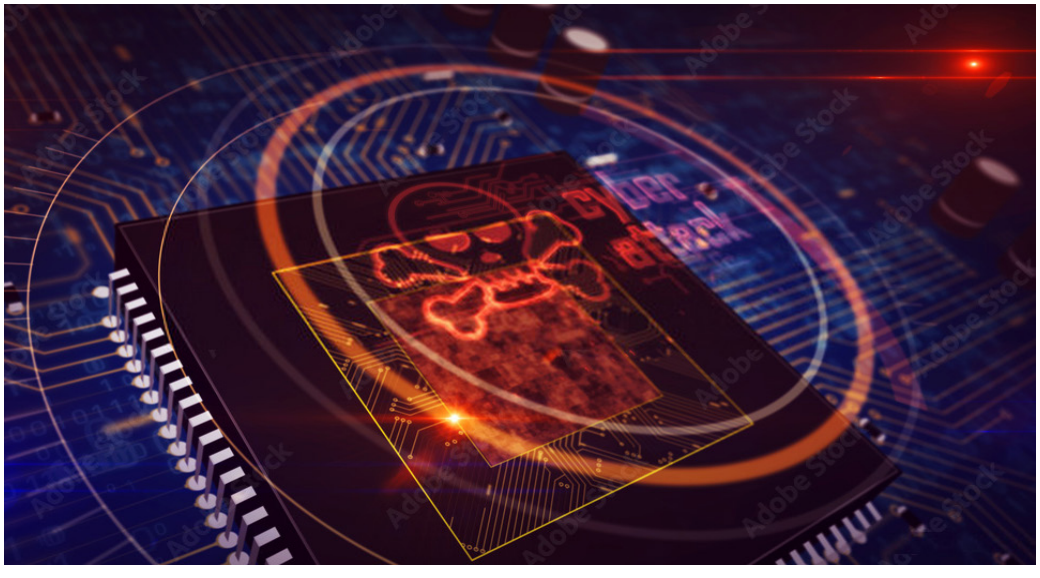
COMMENTARY

New Power Paradigms?

Artificial Intelligence and Cybersecurity as Protean Security Disruptors

Dr. Stephen Nagy

Dr. Phar Kim Beng



Abstract

As we enter the Age of Artificial Intelligence and an increasingly securitized cyberspace, the direction of history, materially or ideationally, may be diverging away from those articulated by Francis Fukuyama, Parag Khanna, and Yan Xuetong. This will impact how we conceive of great powers and leadership, as new forms of power and the creation of power manifest not according to human logic and capacities but instead according to artificial intelligence (AI) algorithms. AI and cybersecurity have become protean security disruptors and may manifest into new power paradigms for states and nonstate actors.

***

The basic rudiments the of Internet were originally called ARPANET. It was designed for the Pentagon and other military scientists' computers to remain functional and reach out to one another in the advent of a nuclear

exchange between the now defunct Soviet Union and the United States. In this scenario, the President of the United States (POTUS) would be hidden or sheltered. If he did not survive the initial nuclear strike, ARPANET would provide the digital infrastructure to enable his vice president to be immediately sworn in by one of the nine judges of the US Supreme Court to be the successor. In either case, there would be a POTUS to fill in any "political vacuum," as stated in the US Constitution and elaborated in the amendments under the US Bill of Rights.

The Internet became a major force after the end of the Cold War, as marked by the fall of the Berlin Wall in 1989, and the disintegration of the Soviet Union on 26 December in the following year. It was assumed by many triumphalist US scholars that the US had won. Among the prominent defense intellectuals and scholars of this mind-set was the late Charles Krauthammer, a columnist with *TIME* magazine, who called the new geopolitical landscape the "Unipolar Moment" in 1990.[1] In turn, the late Samuel Huntington, who wrote in the pages of *Foreign Affairs* in 1993, affirmed that the new world order was defined by a "Uni-Multipolar System," where the United States would be the first among equals,[2] while other permanent members of the United Nations Security Council (UNSC) would have to oblige themselves to Washington's foreign policy whims.

This unequal hierarchy was embodied in Francis Fukuyama's 1989 *National Interest* article "The End of History?," even though he has since conceded that he had been overly exuberant with his essay,[3] originally based on the Hegelian Dialectic of human history moving according to the teleological "Geist" (spirit), or, more precisely the "elan of the time."

Over the course of the next three decades, world events would prove these analyses to be erroneous. Parag Khanna's essay on "The New 'End of History'" argues that "The rise of Asia presents the strongest evidence for geopolitical entropy as the new arc of history, both material and ideational."[4] Chinese scholars—such as Tsinghua University's Yan Xuetong, in his works *The Transition of World Power* and *Leadership and the Rise of Great Powers*— argue that rather than a teleological view of human history, domestic and global leadership are based on moral-realist explanations combined with classical Chinese political theory. Yan argues that leadership, not events, account for the emergence (and decline) of great powers. Borrowing Yan's logic, the United States could have won the Cold War either because of its own leadership or due to the dysfunctional leadership of the Soviet Union—or both.

As we enter the Age of AI and an increasingly securitized cyberspace, the direction of history, materially or ideationally, may be diverging away from those articulated by Fukuyama, Khanna, and Yan. This will impact how we conceive of great powers and leadership, as new forms of power and the creation of power

manifest not according to human logic and capacities but instead according to AI algorithms and the opaque cyberspace that we have become dependent on. In a sense, AI and cybersecurity have become protean security disruptors and may manifest into new power paradigms for states and nonstate actors.

For example, recent cybersecurity attacks of multiple forms against the public and private sectors of the United States, including its energy pipeline as recently as 10 May 2021,[5] have highlighted the increasing salience of asymmetric power as manifested in cyberattacks on government institutions, businesses, and even health infrastructure. These were also ransomware attacks, equivalent to blackmail. If a certain amount of money is not paid to the hackers, cyberattacks on the firms would be escalated to paralyze the whole operation at the touch of the hackers' keyboards. IBM X Force even identified ransomware as the number one threat among the top ten cyberattacks.[6] In 2021, when nine US meat factories were all subjected to what seems to be a coordinated Russian attack, it demonstrated that the threats to the United States or others' cybersecurity can fluidly and repeatedly run from state to nonstate actors.

The number of states and nonstate actors involved in cyberattacks is wide ranging and numerous. The Center for Strategic and International Studies' (CSIS) Strategic Technologies Program provides a detailed list of cyberattacks from 2006 to 2021, such as the June 2015 attacks on the Office of Personnel Management.[7] The first identified attack resulted in the loss of 4.1 million records. The second resulted in the loss of 21.5 million records; 19.7 million of these involved background investigation records for cleared US government employees.

Cyberattacks conducted by state and nonstate actors affect their targets in an asymmetrical way. For instance, a report from Chainanalysis said that North Korea stole around $400 million worth of digital assets in 2021 through seven attacks on cryptocurrency platforms.[8] In January 2022, the cyberattacks conducted on the Ukrainian government were an opening salvo in Russian operations against its neighbor.[9] These examples indicate that cyberattacks will continue to be a tool for anyone conducting disruptions in economic and hybrid warfare.

While a prime target, the United States is far from being the only focus of cyberattacks. For instance, in December 2021, attackers targeted several Southeast Asian states over a nine-month period using custom malware linked to Chinese state-sponsored groups.[10] These attacks are assumed to be linked to territorial disputes with China in the South China Sea. Emerging and smaller states are not well situated to deal with cybersecurity. To consolidate the cybersecurity of the 10 member states of the Association of Southeast Asian Nations (ASEAN), the European Union (EU) agreed to provide 2.5 million Euros from 2018 to 2020 to consolidate the cybersecurity of the regional organization,

The cybersecurity company Sophos' *State of Ransomware 2021* survey, which was conducted in January and February 2021, interviewed 5,400 information--technology (IT) decision makers in 30 countries around the globe.[11] These nations shared one commonality: they are either developed or developing countries that have large, medium, and small companies with varying degrees of vulnerabilities and the ability to pay the ransom. Even if the ransom is paid in full, there is no guarantee that cyberattacks will stop. This perpetuates a cycle of incentives to keep the attacks dormant but still actionable in the future.

Whether it was due to ransomware attack or not, the vectors of breaches are unrelenting. Massive wealth gained through repeated blackmail is increasing.[12] Some Russian and Chinese hackers enjoy the backing of their respective governments. When the cyberattackers are caught red handed, the predators and their state promoters mutually deny any links. Such links, however, can be proven in courts of law. However, this niche area of law will ensure the legal fees are perennially high, invariably leading to a double jeopardy for the hapless victims.

Thus, one must not discount the fact that some companies do prefer to keep these acts unreported to prevent a further and wider sabotage. Hence, under--reporting cybersecurity breaches is a fact of the postmodern landscape; where one's personal information, such as identity, image, video, audio (potentially altered by deep fake technology), and compromised passwords on all electronic devices—especially those connected to the Internet of Things (IOT)—will become a sad fact of life; especially if the person or corporate entity is subject to constant phishing, harassment, and bullying. The sum of these acts can lead to a permanent loss of income and privacy or even the deterioration of mental health, leading to various psychological disorders and, potentially, suicide.

Ironically, the behavior of these modern-day cyberbuccaneers, for the lack of a better analogy, do resemble the early machinations of European pirates in the fifteenth century. States often paid the pirates who roamed the seven seas to not attack the ships carrying their treasures—spices, gold, slaves, and more—that were returning from their long journeys.

Over time, a twin combination of patriotism and macabre profiteering were fused into a complete yet distorted whole, where these pirates became mercenaries of the state and mercurial traders of their own under the pretense of defending their queens and kings. In exchange, the throne would issue a "letter of marque and reprisal," from the countries of their origin, to showcase their jingoistic patriotism by looting the ships of other countries instead. Sir Francis Drake was one such example during the Elizabethan Age. Such confidential agreements represented a win-win scenario for the throne and the privateer. Ahmed Hirsi said, "pirates are not fish; they don't live in the sea, they live in the cities."[13]

For the long term, the threat of a cybersecurity attack and AI being deployed in malevolent fashion is now a permanent feature of the international system. It has gone from offline to online, especially during the pandemic when billions work from home, information is shared over cloud-based platforms, and one account is linked to other devices.

In short, the pervasiveness and dependency on cyberspace for commerce, communication, and collaboration together with the integration of AI algorithms into all our digital devices represent twenty-first-century digital Trojan horses. Likewise, the growing number of state and nonstate actors exploiting these technologies for financial and or geopolitical gain magnifies the protean nature of AI and cyberspace and highlights their potential to disrupt all aspects of our hyperconnected world.

Dr. Stephen Nagy

Dr. Nagy (nagy@icu.ac.jp) is a senior associate professor at the International Christian University in Tokyo, a senior fellow with the MacDonald Laurier Institute (MLI), a fellow at the Canadian Global Affairs Institute (CGAI), and a visiting fellow with the Japan Institute for International Affairs (JIIA). Twitter handle: @nagystephen1.

Dr. Phar Kim Beng

Dr. Phar is the founder and CEO of Strategic Pan Indo-Pacific Arena. He is a regularly featured writer for *The Jakarta Post* and was the former Director of Political and Security Community in ASEAN Secretariat, a former visiting fellow with the Japan Institute for International Affairs (JIIA, 1999), and an associate fellow of edX, an online learning platform pioneered jointly by Harvard University and MIT since 2016.

Notes

1. Charles Krauthammer, "The Unipolar Moment," *Foreign Affairs*, 18 September 1990, https://www.foreignaffairs.com/.
2. Samuel P. Huntington, "The Lonely Superpower," *Foreign Affairs*, March-April 1999, https://www.foreignaffairs.com/.
3. Francis Fukuyama, "The End of History?," *National Interest*, no. 16 (Summer 1998): 3-18, https://www.jstor.org/.
4. Parag Khanna, "The New 'End of History'," *National Interest*, 6 March 2021, https://nationalinterest.org/.
5. Tim McDonnell, "Energy companies are the firms most likely to pay cyberattack ransom," *Quartz*, 11 May 2021, https://qz.com/.
6. "IBM X-Force Threat Intelligence Index," *IBM*, https://www.ibm.com/.
7. "Significant Cyber Incidents since 2006," *Center for Strategic and International Studies*, https://csis-website-prod.s3.amazonaws.com/ .
8. "North Korea hackers stole $400m of cryptocurrency in 2021, report say," *British Broadcasting Corporation*, 14 January 2021, https://www.bbc.com/.
9. Jenna McLaughlin, "Russia could cyberattack Ukraine – again – and disrupt the entire world," *National Public Radio*, https://www.npr.org/.

10. "Significant Cyber Incidents since 2006," *Center for Strategic and International Studies*, n.d., https://csis-website-prod.s3.amazonaws.com/.

11. Sophos, "The State of Ransomware 2021," *Sophos*, April 2021, https://secure2.sophos.com/.

12. Luke Irwin, "The 5 biggest ransomware payouts of all time," *IT Governance* (blog), 18 May 2021, https://www.itgovernance.co.uk/.

13. Jean Edmond Randrianantenaina, "Maritime Piracy and Armed Robbery against Ships: Exploring the Legal and the Operational Solutions. The Case Of Madagascar," *Division for Ocean Affairs and the Law of the Sea, Office of Legal Affairs*, *United Nations*, https://www.un.org/.

Disclaimer