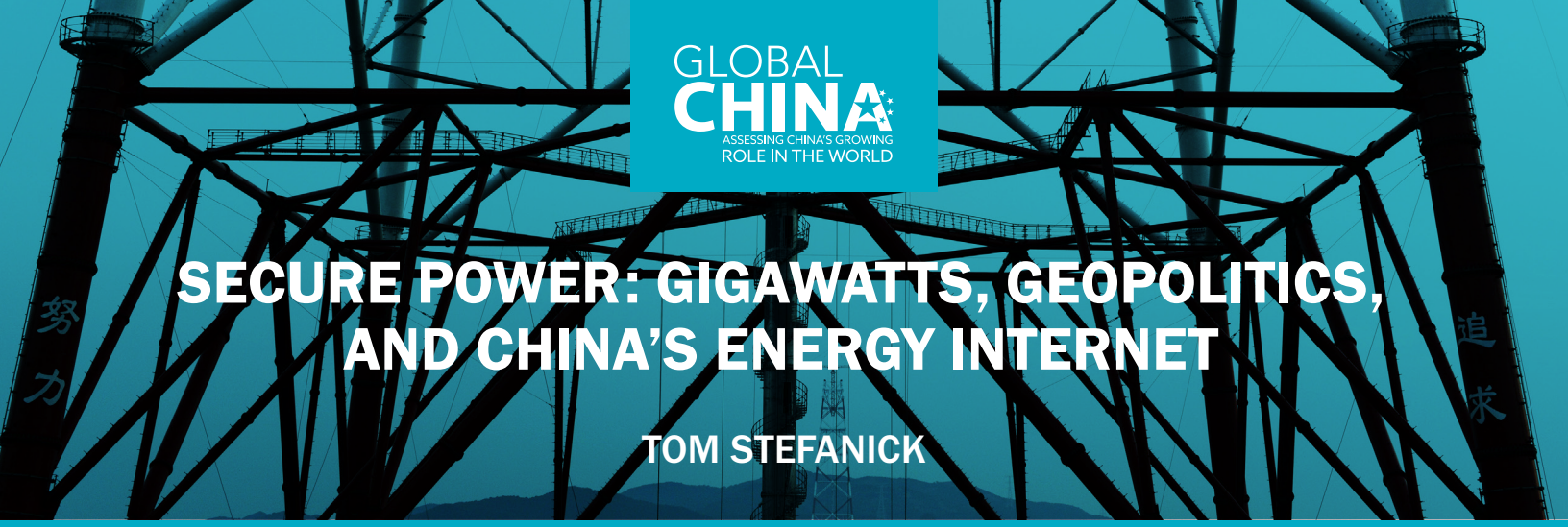

SECURE POWER: GIGAWATTS, GEOPOLITICS, AND CHINA'S ENERGY INTERNET

TOM STEFANICK

APRIL 2020

EXECUTIVE SUMMARY

The importance of China's electrical grid is growing in scale and complexity as it supports economic growth, integration of renewable energy sources, and the geostrategic goals of the Belt and Road Initiative (BRI). China's planned shift from electricity production largely based on coal-fired generators to a combination of hydropower, wind, solar photovoltaic, and gas generators is occurring in tandem with a shift to a market-driven electricity system. These changes introduce enormous technical complexities to what is in effect the largest interconnected machine on Earth. Complex electrical networks require continuous automated monitoring and control. The use of devices connected between the grid and the internet has proven to be a very cost-effective means of providing that control, but those internet connections expose physical electric power equipment to risks of cyberattacks like the ones executed in 2015 and 2016 against Ukraine. China is trying to build resilience into its electrical grid through a combination of training, management, and technology.

The second of these two cyberattacks on Ukraine's electrical grid, in 2016, demonstrated how a malevolent actor in cyberspace could destroy physical components of the grid, thereby disrupting water supplies, hospitals, and food distribution. Since many of these physical devices that enable electricity flows are massive, difficult to replace, and expensive, their destruction can lead to extended power outages and widespread human suffering. Both the U.S. and China are deeply concerned about the resilience of their grids against such attacks. China's approaches to securing their grid, like those of the United States, involves a mix of guidance, regulation, personnel training, and technology. A review of two of the most widely discussed emerging technologies — quantum communications and artificial intelligence — suggests that neither of these will provide robust solutions to grid protection in the next 10 to 15 years.

China's efforts in cyberspace to steal information from U.S. companies and conduct espionage against U.S. military networks are being met by a more forward-leaning U.S. defense that may include defensive operations within Chinese hacker networks. This forward defense posture has been articulated in several U.S. strategy documents. However, the U.S. makes clear that peacetime attacks on civilian infrastructure is not part of the strategy. This important distinction between networks hosting malicious hacking, and networks used to control civilian infrastructure must be clearly understood as cyber policy evolves.

Given the mutual concerns of the U.S. and China over the security of their electrical grids, there may be an opening for mutual agreement for restraint from potentially-threatening behaviors within each other's grid networks. Such an agreement could build on a broader set of principles discussed several years ago with the Chinese, regarding potential restraints from certain behaviors in civilian infrastructure more broadly. Furthermore, an agreement could be crafted that does not logically interfere with the U.S. forward strategy in cyberspace. Such an agreement could provide a useful component of U.S. and Chinese grid security, and a basis for stable interaction in the event of a crisis.

INTRODUCTION

The electrical grid is a technological key to many Chinese national goals: economic development, social stability, pollution reduction, and energy independence via increased use of wind and solar energy. In addition, electricity is an element in China's ambitious efforts to broaden its geostrategic reach by interlinking energy systems with other countries. Like trade and other infrastructure agreements, electricity networks can be used as tools of influence.[1] By investing in electricity generation, transmission, and distribution in developing countries, and linking the Chinese grid with those other countries, China can simultaneously win support from local elites, help stimulate new markets for trade, and diversify the sources of electrical power to help stabilize its own grid. In addition, by introducing Chinese experts and equipment into these international projects, China can accelerate the diffusion and adoption of its own technical standards into other countries. Setting standards for specialized electric power equipment in a way that favors Chinese manufacturers can help increase the market share for those companies.

Expansive physical power grids come with cybersecurity risks of enormous consequence, however. This paper reviews how Chinese experts view some of the emerging cybersecurity risks to their grid, and how they have responded at two levels: top-down guidance from key organizations and leaders, and the bottom-up push of research and development (R&D) themes emerging from universities and enterprises, in particular the massive State Grid Corporation of China. The high-level guidance documents demonstrate that the Chinese leadership is greatly concerned with the risk of cyberattacks on the electricity grid, and shows how they try to address this concern by pushing to clarify the roles and responsibilities of the various players. The technical journals on the other hand, reflect the very broad range of basic and applied research related to cybersecurity on China's grid. While I focus in this paper on quantum secure communications and artificial intelligence (AI) as two emerging technologies that are very prominent in U.S. policy discussions, it was clear that these two technical themes were by no means dominant in the Chinese research literature.

As China continues to extend their electricity grid within and beyond their borders, they will be forced to address the tension between greater reliance on the internet to run the grid and greater risk of attack. In the midst of active competition between the U.S. and China in a cyberspace teeming with malicious actors, there may be enough mutual concern about the resilience of the power grids to provide the basis for some form of agreement on mutual restraint. Given the complexity of cyberdefense of electrical grids, it would be useful for both the U.S. and China to have some mutual reassurance in time of crisis that the other major world power was exercising restraint in this domain. I will discuss a narrow set of terms for agreement between the U.S. and China to avoid broad cybersurveillance activities as well as active cyberattacks in electricity networks.[2]

In addition to U.S. concerns regarding its own electrical grid, there are deep and long-standing concerns over China's use of the internet for spying, stealing commercial property, and attacks on military networks. These topics, as well as China's internal censorship, have been addressed in great detail elsewhere.[3]

THE LARGEST MACHINE IN THE WORLD

Operating continental-scale power networks requires tight integration of massive high-voltage generators, transformers, and cables on the one hand, and precision real-time sensing, synchronization, and control on the other. Data networks are critical to enabling human and automated control of power grids through devices often referred to as supervisory control and data acquisition (SCADA) systems.[4] The complexity of modern grids arises from several fundamental features of large electricity networks:

- The location of power generation may be hundreds or thousands of miles from where it is used. This is particularly true in China, where expansion of wind and solar power is expected to take place largely in the northern and western provinces, far from the main population centers in the east.

- Demand for energy by industry, transportation, household, and other users varies widely over the course of a day as well as on other time scales. However, energy supply must always be capable of meeting the peak demands for homes, schools, hospitals, and factories to function safely and efficiently.
- Electricity must be used the instant it is produced, but it is very difficult to quickly adjust generation rates based on changing demands. Modern grids sometimes integrate storage methods to partially smooth this variability: from electric vehicle batteries in homes to pumped storage facilities.
- Renewable energy sources such as wind and solar power vary with time, often unpredictably, and generally do not align with the time of electricity demands. Nonetheless, there is a top-down push in China to significantly increase the proportion of renewable sources on its grid.
- Energy generated by small-scale producers, including homes, needs to be introduced into the electrical grid in a way that benefits all parties. Guaranteed access to selling power on the grid makes electric vehicles more economic for homeowners by enabling batteries to store and release energy, and creates incentives for investors to establish wind and solar power generators.
- The electricity supply to all users must be highly reliable, and robust to random events such as generator outages, loss of transmission lines, solar flares, and malicious attack.

Connecting thousands of electricity producers and millions of electricity consumers operating on independent schedules requires constant redirection and split-second synchronization of electricity storage, routing, and transmission. Modern electrical grids use both direct current and alternating current for production, transmission, and end use. The more common alternating current (AC) is so called because its current and voltage are constantly varying as a regular wave form that changes from peak to trough back to peak in a few milliseconds. The relationship between two different AC wave forms in time is called their phase. When attaching an AC source to another part of the grid operating on AC, the phases of the two different AC systems must match very closely. Without precise alignment of the phases, power can be reduced and even severe equipment damage can occur. Direct current (DC), on the other hand, does not vary with time, so connecting DC systems with other DC systems does not require this same level of synchronization. In addition, very high-power DC transmission suffers less energy loss than AC power does over long transmission distances, whether on towers, in buried cables, or even underwater. Interconnecting high-power AC and DC transmission grids together requires conversion from one type of current to the other. Large, expensive special equipment is required for this conversion, and Chinese companies have become some of the world leaders in developing ultra-high-voltage (UHV) devices for efficient long-distance transmission.

Electrical grids require continuous adjustment of power flows due to the random behavior of devices that they connect, so controllable and flexible electricity production is critical to most grids. Large gas-fired electricity generating stations are the most flexible, while coal-fired plants are less so. China depends on coal-fired plants for about 60% of their electricity, though the government is working to reduce that fraction, as I will discuss later. There is a drive in China to move toward renewable energy in order to reduce carbon dioxide emissions as well as enhance energy independence. Hydroelectric power is China's largest source of renewable power, providing about 20% of its electricity, and is a relatively controllable and predictable source of renewable AC power. In order to create economic incentives for investments in other renewable energy sources such as wind turbines and DC photovoltaics, the grid must be capable of integrating these sources into the main grid, paying a market price for them, all the while adapting to the inherent variability and unpredictability of these sources. Combine the complexity of supplying power, with the randomly fluctuating electricity demand from millions of large factories and homes, and it becomes clear why modern electrical grids require constant control even under ideal conditions. However, accidents frequently require the grid to adapt.

On August 14, 2003 there was a blackout in the northeast United States that left 50 million people across eight states and Canada without power for

more than a day. The massive blackout was initially triggered by trees touching power lines in Ohio, but soon cascaded outward in spite of desperate attempts by power company professionals to contain it.[5] The impact left people stranded as transportation systems shut down, and basic services stopped.[6] When a part of the grid goes down without warning, it is difficult to simply switch excess capacity to cover the loss, for the reasons described above. Sudden changes in power levels in one part of the grid can create damaging effects in other sub-grids, and these can propagate outward as they did in the 2003 blackout. Chinese research on electrical grid control often cite the 2003 blackout as a milestone in their own thinking about linking the internet with the grid in order to stabilize it. China's own experience includes a 2008 blackout in south China caused by a snowstorm, which caused power outages for 14.7 million households.[7] Large electrical grids deal with minor outages on a daily basis, and while the vast majority of these can be contained, the numbers are increasing. With the rapid expansion of the internet and its increasing reliability in the 1990s, the idea of using it to monitor and control the electricity grid was a natural technological development offering tremendous benefits.

Along with these benefits, however, links between the high-voltage infrastructure and data networks open pathways to cyberattack, such as the two Russian cyberattacks on the Ukrainian power grid. A review of these two attacks highlights the rapid and dangerous trend in cyber-attacks on electrical grids. The first attack occurred in late December 2015 and the second in late December 2016, but both were preceded by months of undetected activity within the power company network by the attackers. Both attacks demonstrated the effectiveness of long-term reconnaissance of the internet infrastructure, the SCADA systems, and use of diverse methods to confuse or bypass human operators in the midst of the attack. The attackers demonstrated a rapid increase in sophistication between the two attacks: In December 2015, the attackers used manually-operated remote control takeover of the human-machine computer interfaces in Ukraine to actually cut power, while in December 2016 the power was cut using automated algorithms. In addition, the December 2016 attack included code designed not only to cut the power, but to destroy physical infrastructure.[8] The use of cyberattacks to damage expensive and often hard-to-replace machines on the grid greatly raises the potential consequences of such attacks on society.

Incentives for adversaries to disrupt electricity grids have been incorporated into many scenarios.[9] For example, the disruption of troop movements and military supply transportation through a nation during the build-up to a crisis would blunt the flow of forces into a theater of war, and would also create confusion on the home front. The cost to the attacker of such a cyberattack on logistics would be negligible compared with the military impacts during an escalating crisis.[10] While the duration and geographic extent of such outages targeted on logistics could probably not be perfectly predicted, given the uncertainties in the behaviors of interconnected electricity sources, such attacks could generally be localized. There are some reports from China of cyberattacks and malware injections in their critical electrical grid systems associated with specific hydropower dams, including the Three Gorges Dam, though none attributed to state sponsorship.[11]

China, like the U.S., worries about the risks and potential consequences of cyberattacks on this critical infrastructure, but also view these risks is as something that must be managed in order to meet the requirements for stable power. Chinese experts in infrastructure concur with their Western counterparts that electrical grids are dynamically linked to the behavior of natural gas, water, oil, and transportation infrastructure.[12] Attacks on the electricity grid will quickly ripple outward to threaten the delivery of basic human needs.

CHINA'S ENERGY INTERNET: GUIDANCE FROM THE TOP

China is in the midst of steady growth in the use of electricity, together with a dramatic shift in the sources of its electric power. China's recent Five-Year Plans (FYP) each include a five-year plan for energy and the electricity sector. The 13th FYP (2016-2020) calls for continued growth in overall generation, as well as major shifts from coal-fired power to wind, solar, and hydro-electric power as a percentage of generation.[13] China is now the world's largest electricity producer by far, producing over 70% more electric energy in

2019 than did the United States.[14] China's growth in electricity production is a recent development, however. In 1990, it was in fourth place in generating electricity, producing less than Japan and Russia, and less than 20% of what the United States produced. China's production of electricity has grown dramatically since then, accelerating in 2002 to overtake the U.S. in 2011.[15]

The growth of China's electricity generation was coupled to the expansion of electricity to rural areas and increased capacity to the heavily populated regions. To get a sense of the complexity of China's grid, consider that China has almost 1.9 million kilometers of high voltage (35,000 volts and above) transmission lines, and close to 13,000 hydro and thermal power-generating units each over 6 megawatts (MW).[16] Coal is projected to account for around 60% of China's electricity generation by the end of 2020, falling below 30% by 2050, while electricity from wind and solar are projected to rise from about 12% in 2018 to 42% in 2050.[17] The western and northern provinces of Inner Mongolia, Yunnan, and Xinjiang are among several significant net electricity exporters to the east of China, with Xinjiang providing about 87 gigawatts of power, over a third of which is produced by wind and solar.[18] Moving all that power over hundreds of kilometers while minimizing power losses requires ultra-high voltage transmission technology, a field in which China is now the leader.[19] The search for reliable renewable power is also leading China far beyond its borders: China's 2018 Arctic Policy calls for development of wind and geothermal energy production in the Arctic,[20] with initial planning set for 2020.[21]

Control of grids through internet connections to centralized human control centers has given rise to a several terms, one of the earliest of which was called smart grid. In the U.S., Smart Grid now refers to Department of Energy programs as well as a group of technologies.[22] Chinese writers also use the term, and in addition articulate a next-generation vision for the smart grid which they call energy internet (EI). The energy internet concept includes sensing and control of the actual electricity grid and its users as discussed above, but in recent years the scope of EI terminology has grown to encompass sensing and control of the energy sources that feed electrical generators such as coal and gas. The concept is also central plans for "smart cities" controlled by the Internet of Things (IoT).[23] Energy internet concepts also include information flows that can be used to send price and market signals. During periods of high demand, for example, prices in an electricity market with limited supply could rise, and industrial users could use that price information to shift power-intensive processes to times of lower-priced power. In 2015, the Chinese Communist Party (CCP) Central Committee and the State Council mandated that electricity grid operators were required to support market and price reforms of the electric power system.[24] The goals of this policy were to improve the pricing, trading, generation, distribution and sales of electric power through improved institutions.[25]

China's national goals for the energy internet have been published for a number of years. In April 2016, the National Development and Reform Commission and National Energy Administration (NEA) published an action plan for China's the energy internet through 2030. The first phases of pilot projects are in the process of changing over to implementation of the energy internet in 2019.[26] They also emphasize the need to track risks to SCADA systems continuously, regardless of whether there is an apparent attack.[27] The lessons from the attacks on Ukraine's power system have clearly been absorbed at the highest levels in Beijing.

> **"China's concerns over the security of its grid are wrapped within a broader national concern about cybersecurity at the highest level.**

China's concerns over the security of its grid are wrapped within a broader national concern about cybersecurity at the highest level. In 2014, China established the Leading Small Group for Cybersecurity and Informatization headed by Xi Jinping himself, bringing together a number of powerful ministries and bureaus and including the People's Liberation Army (PLA). In 2018, the body was upgraded as the Central Commission for Cybersecurity and Informatization.[28]

High-level guidance on cybersecurity specifically for China's electrical grid places the emphasis on management and personnel, ensuring that all organizations involved in electricity grid enterprise take responsibility for protecting the grid. The high-level guidance reviewed here does not delve into the technical details of implementation. Absent from these documents about energy internet security is the kind detailed technological wish list promulgated in the 2017 "Next Generation Artificial Intelligence Plan" issued by China's State Council.[29] This document does refer very briefly to the use of AI in developing the energy internet and energy coordination, but the smart grid is not one of its central themes.

A December 2019 article in China Information Security Magazine provided a useful review of high-level Chinese guidance related to security on the energy internet, grouped into three themes: top-level design and management of the EI, technology improvement and innovation, and use of exercises to train personnel to defend the energy internet. [30] Below is a sample of the range of recent guidance and activities surrounding China's emphasis on grid security:

- In September 2011, the Ministry of Industry and Information Technology (MIIT) issued a notice pointing out the importance and urgency of strengthening the network security management of industrial control systems, specific management requirements, and the urgent needs of system construction and organizational leadership.[31]
- In May 2012, the State Council issued guidance which reinforced the need to strengthen the industrial control system in important areas such as the power system and regularly conduct safety inspections and evaluations.[32]
- In 2016, the "Cyber Security Law" was promulgated, instituting regulations for conduct of cybersecurity drills. It mandated that operators of critical information infrastructure should "develop emergency response plans for cybersecurity incidents and conduct regular drills." Since 2016, Guizhou, Guangdong and Zhejiang provinces have organized network attack and defense exercises. MIIT has been holding energy internet protection competitions, with offensive and defensive teams.[33]
- In 2018, China released the "White Paper on 5G Powered Smart Grid Applications," which elaborated five typical 5G smart grid applications, including intelligent distributed distribution automation, demand side response to electricity load, distributed energy regulation, and advanced metering.[34]
- At the beginning of 2019, the State Grid of China proposed the concept of ubiquitous power Internet of Things. By 2024, the ubiquitous power IoT is intended to be fully completed to form the energy internet ecosystem, controlling all aspects of energy production, transmission, and consumption in real time. The following year, China Southern Power Grid released the "Digital Transformation and Digital South Network Construction Action Plan (2019 Edition)."[35]

SECURING CHINESE SMART GRIDS

China's efforts to make their energy Internet more resilient parallels the recommendations from Richard Clarke and Robert Knake in their recent book *The Fifth Domain*, in which the authors state their position as: "We want to make our defenses so good, and our architectures so strong, that we do not care whether we are being attacked most of the time because the attacks have no serious effects."[36] China's energy and cybersecurity researchers — often funded by the State Grid Corporation of China — have been working on a wide array of technical approaches to securing their grid from cyberreconnaissance or cyberattack.[37] I will address only two of them here, which are still considered emerging technologies by most experts, but which typically receive a great deal of attention in Western policy discussions: *quantum* — communications technologies that use the properties of quantum physics to improve the secure control of electricity grids — and *artificial intelligence* — the use of algorithms to detect cyberattack patterns in order to protect systems.

It is important to keep in mind that China's efforts in these and other technical areas of grid defense — like those of the U.S. — are not framed within the context of a race for supremacy. The inherent technical challenges of maintaining and growing an electrical grid the size of China's are sufficient to drive the intensive R&D efforts.

CHINA'S APPLICATION OF QUANTUM KEY DISTRIBUTION AND THE QUANTUM INTERNET TO SMART GRIDS

China's emphasis on applications of quantum physical phenomena with respect to communications security certainly aligns with their interest in energy internet security, as well as the wider desire for communications security. In their review of China's trajectory in quantum technologies, Elsa B. Kania and John K. Costello point repeatedly to the profound impact that the classified information leaked by U.S. National Security Agency subcontractor Edward Snowden had on China's emphasis on quantum communications:

> "Snowden's revelations detailed the extend of U.S. intelligence capabilities and have evidently intensified the Chinese leadership's anxieties regarding China's domestic information security and its susceptibility to cyber espionage and influence. This incident has been so fundamental to Chinese motivations that Snowden has been characterized as one of two individuals with a primary role in the scientific 'drama' of China's quantum advances, along with Pan Jianwei, the father of Chinese quantum science."[38]

China's 13th Five-Year Plan (2016-2020), which was developed following Snowden's revelations of U.S. capabilities, raised the prominence of quantum information science as a national strategic requirement. China is now building the National Laboratory for Quantum Information Science, the largest centralized quantum research facility in the world.[39]

China has been investing steadily in the three main areas of quantum information science — quantum communications, quantum computation, and quantum metrology — since 1998. A recent review of Chinese research and development in all three areas concludes that it is quantum communications, especially quantum key distribution (QKD), that will be the first technology that is applied.[40] This assessment is based on the success of parallel efforts in China to demonstrate satellite-to-ground QKD and intercontinental quantum secure communication with the Micius satellite, as well as terrestrial systems that can send quantum-secured keys over the 1,100 kilometers between Beijing and Shanghai.[41] While this research supports commercial, military, and government security interests, the potential of QKD for improving electrical grid security generates significant interest. The State Grid Corporation of China funds research in this field, and has its own laboratory for QKD research.[42] Chinese scientists have been making steady progress, and have been addressing some of the potential weaknesses of the new technology.[43] A recent study by leading Chinese quantum experts forecast that "we can expect in the next 10-15 years quantum repeater technology will be extensively developed and a quantum repeater link (>500 km) could be built."[44]

It is helpful to distinguish how quantum secure networks might be used for defense, intelligence, finance, and government secrets on the one hand, and energy internet applications on the other. Transmitting state secrets, financial information, or personal data does not usually depend on split-second timing in the way that industrial control systems and SCADA systems do. Energy internet applications often require communications over large distances, under harsh environments, and with tight constraints on delays and latency. Chinese researchers working to apply quantum secure information flow to the energy internet are realistic about the prospects and address a number of very practical issues. For example, given the hundreds of kilometers spanned by many power transmission lines, some fiber optic links must be strung over high towers spanning mountains with high winds. The resulting stress and vibrations can degrade the photon polarization states which carry the quantum information.[45] Systematic studies of many technical alternatives for increasing the range of quantum communication lines are ongoing within China, and the research indicates that there is no single path toward long-distance quantum communications for the power grid.[46] It would seem likely that widespread adoption of quantum secure communications would appear first in applications that can ensure relatively noise-free communication channels, such as metropolitan fiber optic networks and space. Even these applications will probably require on the order of 10 years before they are widely deployed. Energy internet security based on widespread use of quantum communications methods is likely to require more than 10 years to be adopted.

APPLICATION OF ALGORITHMS IN SMART GRID SECURITY

The definition and scope of the term "artificial intelligence" has been in constant flux over recent decades, and today, the use of the term can be stretched to include a wide variety of automated algorithms that have some feature of adaptation, inference, pattern recognition, or autonomous control. China's embrace of artificial intelligence includes national efforts to apply AI to their electrical grid: the stated goal of the Cyberspace Administration of China is that "By 2024, the ubiquitous electric power Internet of Things will be built to fully realize business collaboration, data penetration, and unified IoT management, and form an energy Internet ecosystem that builds together, governs and shares" through the application of artificial intelligence.[47] These Chinese AI pronouncements are largely aspirational, however. Hopes that AI will improve grid performance are varied in the U.S., with some utility industry experts indicating that we are in the early stages of using data analytics for power management and that it is not practical to implement AI currently.[48]

> **"Chinese researchers often cite the attack against Ukraine's power grid as a starting point for analyses of threats.**

Automated algorithms for controlling electrical grids, for attacking them, and for defending them are all under development simultaneously.[49] A particularly rich class of targets for malicious AI are the types of automated control systems that are used to control electrical grids.[50] There are a number of approaches for attacking a smart grid through the cyber-physical systems that sense or control electricity via internet signals. Simply turning off the sensors is likely to be noticed, so a more subtle means would be to slowly modify the data coming out of sensors, or modify the data as it enters the controllers. One of the ways of disrupting power systems would be to disrupt precision time signals from the Global Positioning System (GPS) or China's similar BeiDou system, since power systems use these signals to measure and synchronize the phase of alternating current.[51] Related methods attack not the sensor data but the feedback control commands by injecting erroneous signals for phase or other control variables, sufficient to destabilize feedback control systems. Chinese researchers often cite the attack against Ukraine's power grid as a starting point for analyses of threats, such as false data injection to confuse automated power controls. These experts also occasionally indicate that, due to the complexity of power systems, the interpretability of AI threat detection systems is "usually poor."[52] Chinese experts also cite the Triton/Trisis attack on a Saudi Arabian petrochemical plant as an important and troubling milestone, as that attack took control of the safety instrumented system that provides emergency shutdown for plant processes that go out of control.[53]

Chinese experts have been researching algorithmic methods for diagnosing, modeling, and suppressing threats to physical systems on the internet, as a brief sample indicates:

- Advanced methods for finding attack paths into the defended network.[54]
- Defensive AI reinforcement learning algorithms can adapt to attacking adversaries that attempt to poison their defensive training. This example of counter-countermeasures is analogous to many military operations in electronic warfare as well as the physical domains.[55]
- Some researchers formulate cybersecurity of critical systems in terms of a continuous adversarial game with close engagement in cyberspace, not unlike the characterization in the U.S. Cyber Strategy. If the defender is to thwart the attacker, it must reconfigure defenses as the attacker learns about them.[56]

Common to all the approaches discussed above is that they are algorithmic in nature and depend on the speed, adaptability, and accuracy of software running on distributed computers to enhance security. The nature of AI defenses against AI attacks leads to a continuous, autonomous game which could unfold too rapidly for any actor to completely control. With the random elements in electrical grid behaviors, the outcome of such games is of course uncertain. Given

the need for high reliability and stability in China's electricity system, AI-based defenses as an emerging technology would appear to carry significant risks.

Automated learning algorithms that can penetrate an adversary's energy internet for surveillance or for cyber-physical attack give rise to an adversarial offense-defense interaction that has particular fascination in the R&D community, and there is a large and growing body of technical research related to automated attack and defense in the cyber domain. However, highly automated tools for power grid surveillance or attack are unwise in application. Any nation concerned about controlling a developing crisis would wish to avoid unleashing algorithms that have unpredictable behaviors into adversary electrical grids that demonstrate unpredictable responses.

I conclude that AI-driven algorithms applied to the grid would be most safely and effectively used for monitoring networks to detect threat behaviors. They may also be used for the much more challenging task of detecting and identifying anomalous behavior that does not fit a known threat. On the offensive side, fully autonomous algorithmic attacks on the energy internet and against SCADA systems are contrary to U.S. and Chinese goals of stability within those technical systems.

CAN THE U.S. AND CHINA LEAVE GRIDS ALONE?

The electrical grid of China remains a critical element for their economy, social stability, and geostrategic goals. With the stakes of energy grid security being as high as they are for China and the United States, it is worth exploring the possibility of an agreement to extend the "off-limits" nature of attacks on electrical grids to broader set of behaviors: avoidance of peacetime active reconnaissance of electrical grids, and of the energy sources that directly support them, such as gas lines and hydroelectric power stations.

While this paper is mainly about China's cybersecurity activities to protect their grid, it is worth quickly reviewing the deep concerns that are driving policy in the United States. The U.S. Navy's Cyber Security Review of 2019 stated:

> "The systems the US relies upon to mobilize, deploy, and sustain forces have been extensively targeted by potential adversaries, and compromised to such extent that their reliability is questionable. Supervisory Control and Data Acquisition (SCADA) systems, strategic and tactical communications, and logistics systems are of uncertain utility given the well-recognized vulnerabilities inherent and threat created in those systems."[57]

> **"Concerns about risks from Chinese attacks on U.S. grids are heightened by the long, persistent espionage that China has been conducting within U.S. networks.**

There are a number of malicious groups targeting the North American electricity grid.[58] Concerns in the U.S. about cybersecurity on the electrical grid are now a well-publicized feature in the current U.S. confrontation with China and particularly with Russia.[59] Doubts about the resiliency of the U.S. grid have led to legislation called the Securing Energy Infrastructure Act that, among other things, calls for U.S. National Laboratories to investigate risks to digital control of the grid, as well as consideration of some non-digital grid control systems.[60] Concerns about risks from Chinese attacks on U.S. grids are heightened by the long, persistent espionage that China has been conducting within U.S. networks. The United States has long been the target of online spying and theft by Chinese hackers: intensive espionage against individuals such as the capture of extensive amounts of sensitive personal data from the Office of Personnel Management (OPM), a wide array of intellectual property theft, and military intelligence gathering. For policymakers, Chinese hacking behavior against the Department of Defense (DOD), their contractors, and OPM is difficult to separate from potential cyberattacks against power grids. DOD strategy documents do make the distinction between entering an adversary's network for the purposes of thwarting attacks on our own, and recognizing the special status of networks that control physical infrastructure such as electricity.

U.S. Cyber Strategy that has been recently clarified through two official documents. These documents exclude the peacetime use of cyberattacks against foreign infrastructure as part of U.S. strategy. The 2018 Department of Defense Cyber Strategy Summary articulates a continuous forward posture coupled with recognition of multilateral discussions on responsible behavior in cyberspace.[61] The DOD Cyber Strategy calls for a posture that can:

- "**Leverage automation and data analysis to improve effectiveness**: The Department will use cyber enterprise solutions to operate at machine speed and large-scale data analytics to identify malicious cyber activity across different networks and systems. The Department will leverage these advances to improve our own defensive posture and to ensure that our cyber capabilities will continue to be effective against competitors armed with cutting edge technology."[62]
- "**Persistently contest malicious cyber activity in day-to-day competition**: The Department will counter cyber campaigns threatening U.S. military advantage by defending forward to intercept and halt cyber threats and by strengthening the cybersecurity of systems and networks that support DoD missions. This includes working with the private sector and our foreign allies and partners to contest cyber activity that could threaten Joint Force missions and to counter the exfiltration of sensitive DoD information."[63]

The 2018 Command Vision for U.S. Cyber Command emphasizes the tactical logic of the forward defense posture set out by the DOD Cyber Strategy:

> "Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins. Continuous engagement imposes tactical friction and strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks. We will pursue attackers across networks and systems to render most malicious cyber and cyber-enabled activity inconsequential while achieving greater freedom of maneuver to counter and contest dangerous adversary activity before it impairs our national power."[64]

A number of U.S. cybersecurity policy experts have raised questions regarding the risks and efficacy of this strategy. However many—including myself—accept the tactical logic of the continuous engagement coupled with increased resilience.[65] In addition, these strategy statements are defined as defending against attacks, and it is reasonable to assume that cyberattacks do not originate from within electrical grid control networks. Therefore, it is reasonable to assume that the forward defensive activity is not directed toward foreign electrical grids.

The quotes above from the DOD Cyber Strategy and the USCYBERCOM Command Vision emphasize on forward engagement with Chinese entities attacking the U.S. While no behavior is explicitly excluded, the DOD Cyber Strategy commits the U.S. to "reinforce norms of responsible State behavior in cyberspace" based on principles developed by the UN Group of Governmental Experts, which "include prohibitions against damaging civilian critical infrastructure during peacetime."[66] U.S. strategy therefore implicitly excludes damaging attacks against Chinese grid infrastructure in peacetime. It does not exclude peacetime reconnaissance and preparation for such attacks.

The distinction between peacetime reconnaissance and peacetime attack are important, and very distinct. Authoritative definitions of cyberspace exploitation and cyberspace attack are provided by the Joint Chiefs of Staff in the Cyberspace Operations Doctrine. In particular, cyberspace exploitation may include the kinds of peacetime reconnaissance and preparations described above within the adversary's networks (red cyberspace) or adjacent to them (gray cyberspace):

> "Cyberspace exploitation actions include military intelligence activities, maneuver, information collection, and other enabling actions required to prepare for future military operations. Cyberspace exploitation actions are taken as part of an offensive cyber operation (OCO) or defensive cyberspace operation-response action (DCO-RA) mission and include all actions in gray or red cyberspace that do not create cyberspace attack effects. Cyberspace exploitation includes activities to gain intelligence and support operational preparation of the environment for current and future operations through actions such as gaining and maintaining

access to networks, systems, and nodes of military value; maneuvering to positions of advantage; and positioning cyberspace capabilities to facilitate follow-on actions."[67]

The U.S. forward, persistent strategy described earlier sends the clear message that the U.S. will use its technical abilities in cyberspace to enter and disrupt those networks that are the source of espionage, theft, information operations, or infrastructure attack on the U.S. or its allies. From this, it should be logical for Chinese to conclude that their networks which host offensive cyberoperations would be targets. Keeping those offensive operations well separated from Chinese electricity, gas, and related information and control networks would be a sensible tactic for avoiding peacetime attacks on those infrastructures. This suggests a tacit set of cooperative behaviors that should be somewhat visible to both sides: If China does not launch offensive cyber operations from networks closely tied to electricity infrastructure, then the U.S. can observe its declared restraint from attacking infrastructure in peacetime, but can continue to attack offending behavior elsewhere in China's networks, per the doctrine. Tacit cooperative behaviors like this — especially if they are reciprocal — may be a basis for a more stable confrontation in cyberspace. This is true in particular since extensive research has demonstrated that deterrence in cyberspace is limited.

It is important to distinguish Russia's demonstrated behavior regarding attacks on power grids with open-source documentation of China's behavior. The Office of the Director of National Intelligence's (ODNI) most recent Worldwide Threat Assessment for Cyber characterizes Russia and China as improving their capabilities directly against the U.S. electricity grid, and points out China's ability to attack gas supply grids that could cut electricity for days or weeks. Whereas the ODNI report explicitly calls out Russia's efforts in "mapping our critical infrastructure with the long-term goal of being able to cause substantial damage," there is no parallel assertion with respect to China.[68] Given the structured and parallel assessments of China and Russia provided in the ODNI's report, these distinctions between Russian and Chinese behaviors with respect to U.S. infrastructure appear to be deliberate. That is, the report's absence of a statement that China is engaged in the kind of broad mapping efforts that Russia is suggests that China is demonstrating more restraint in this area.

Given the indications of restrained behavior on the part of the U.S. and China with respect to the electricity and other infrastructure, a few next steps are worth exploring:

- Declaratory statements from China that parallel the U.S. declaration that infrastructure will not be attacked in peacetime.
- Demonstration from China of additional restraints from mapping and preparing attacks on gas infrastructure, as cited in the ODNI threat assessment.
- Mutual agreement between the U.S. and China to avoid hosting offensive cyberoperations from networks that are closely linked to infrastructure networks.

Over time, both the U.S. and China will continue to ameliorate the risks to their energy grids through technological and operational means. In the meantime, steps such as the ones above provide opportunities to stabilize a subset of the confrontation in cyberspace that already have a basis in current behaviors, and appear to have low risk to each side.

Finally, there is a recent precedent for such an agreement. A broader concept for restraint between the U.S. and China was articulated by RAND Corporation experts and discussed directly with Chinese counterparts in a Track 2 dialogue. That proposal, detailed in a RAND report, received positive response from the Chinese interlocuters.[69] The steps that I am proposing here are more limited and focused.

China's efforts in R&D to introduce emerging technology into protecting their energy internet should not be cast as a "technological race" with the U.S. In the first place, the Chinese already face a range of internet cyberattacks from other entities than the U.S. It can be speculated that as China's geopolitical influence expands — in part driven by its global electrical grid ambitions — it will encounter more groups that want to push back at it as the regional hegemon. China is under pressure to secure its grid, but this is driven by the rapid increase in the importance of electricity to China's economy, as well as the grid's increasing

complexity. China is, in effect, racing against its own internal developments and its growing geopolitical influence.

CONCLUSION

China's generation and use of electricity has undergone dramatic growth over the past 20 years, and is set to continue growing in scale as well as complexity, as sources shift from coal-fired power to more variable wind and solar resources through 2050. This growth in scale and complexity drives requirements for control at all levels of China's grid. Maintaining cybersecurity for the electrical grid is a central concern for both China and the United States. Both the U.S. and China have taken note of the automated, physically destructive attacks by the Sandworm group on Ukraine's power grid SCADA systems. Both the U.S. and China know that improving the standard of living for their people depends on increasingly sophisticated electrical grids controlled by the internet. The U.S. and China also recognize the enormous importance of electricity grids to their abilities to mobilize and operate armed forces in the event of tensions leading to a crisis. China's electrical grid also is part of a larger push toward geostrategic networking throughout Asia, Africa, and beyond. There is a great deal more at stake for the Chinese government and the CCP in securing their grid today than there was even a decade ago.

There are greater mutual incentives for the U.S. and China to agree on restraints from cyberactivities within the other's grid. An agreement on restraint could take several forms, from declarations of restraint from actual attacks on power grids in sovereign territory, to much more restrictive restraints on reconnaissance and surveillance of each other's electricity grid control systems. There might be agreements not to host cyberattacks — say for intelligence gathering or theft of commercial data — from within networks associated with electricity grid control and monitoring. This would allow both parties to conduct defense against such intelligence and theft forward, in the adversary's networks, without creating the appearance of preparing for potential attacks on grids.

Such agreements would provide a basis for limited agreements in a highly contested domain, which would create norms for dealing with crises. As I have mentioned, there is a well-documented precedent for such an agreement. The agreement could be crafted in such a way as to avoid logically conflicting with stated U.S. cybersecurity strategy. Finally, under such agreements, the U.S. could continue to demonstrate resolve in its ongoing competition by using pushing hard against other Chinese activities such as theft, espionage, and information operations, while keeping some areas of negotiation open.

REFERENCES

1 An excellent summary of China's efforts to use electricity as a geostrategic tool is provided by Phillip Cornell, "Energy Governance and China's Bid for Global Grid Integration," (Washington, DC: Atlantic Council, May 30, 2019), https://www.atlanticcouncil.org/blogs/energysource/energy-governance-and-china-s-bid-for-global-grid-integration/; Cornell's blog also references this document from China's Global Energy Interconnection Development and Cooperation Organization (GEIDCO): "Research Report on the Belt and Road Energy Interconnection," Global Energy Interconnection Development and Cooperation Organization, April 2019, https://img1.nengapp.com/tech/ydyl/yjbg_en.html.

2 This proposal is closely is based on one proposed by RAND Corporation experts in 2016: Scott W. Harold, Martin C. Libicki, and Astrid Stuth Cevallos, "Getting to Yes with China in Cyberspace" (Santa Monica, CA: RAND Corporation, 2016), https://www.rand.org/pubs/research_reports/RR1335.html.

3 James Griffiths, *The Great Firewall of China* (London: Zed Books Ltd, 2019); Margaret Roberts, *Censored* (Princeton, NJ; Princeton University Press, 2018); Greg Austin, *Cybersecurity in China: The Next Wave* (Cham, Switzerland: Springer, 2018); Greg Austin, *Cyber Policy in China* (Malden, MA: Polity Press, 2014); Kenneth Lieberthal and Peter W. Singer, "Cybersecurity and U.S.-China Relations," (Washington, DC: The Brookings Institution, February 2012), https://www.brookings.edu/research/cybersecurity-and-u-s-china-relations/.

4 The term industrial control system (ICS) is also used to refer to these devices.

5 To read actual transcripts of the ultimately futile efforts by engineers to control the cascade of failures, as well as a second-by-second account see "Technical Analysis of the August 14, 2003 Blackout" (Princeton, NJ: North American Electric Reliability Council, July 13, 2004), https://www.nerc.com/pa/rrm/ea/Pages/Blackout-August-2003.aspx. Also see "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," (Washington, DC and Ottawa: U.S.-Canada Power System Outage Task Force, April 2004), https://www.nerc.com/pa/rrm/ea/Pages/Blackout-August-2003.aspx.

6 Photographs from New York City republished in The Atlantic on the 15th anniversary of the blackout illustrate the human impact vividly. Alan Taylor, "Photos: 15 Years Since the 2003 Northeast Blackout," *The Atlantic*, August 13, 2018, https://www.theatlantic.com/photo/2018/08/photos-15-years-since-the-2003-northeast-blackout/567410/.

7 Zhaohong Bie, Yanling Lin, Gengfeng Li, and Furong Li, "Battling the Extreme: A Study on the Power System Resilience," *Proceedings of the IEEE* 105, no. 7 (July 2017): 1253-1266, https://ieeexplore.ieee.org/document/7893706.

8 For an exciting discussion of the technology and personalities behind efforts to understand these attacks, see Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Doubleday, 2019).

9 Robert K. Knake, "A Cyberattack on the U.S. Power Grid," (New York: Council on Foreign Relations, April 3, 2017), https://www.cfr.org/report/cyberattack-us-power-grid.

10 Michael O'Hanlon, *The Senkaku Paradox: Risking Great Power War Over Small Stakes* (Washington, DC: Brookings Institution Press, 2019), 171-172.

11 Jason R. Fritz, *China's Cyber Warfare*, (Lanham, MD: Lexington Books, 2017), 24-25.

12 Ibid.

13 Jorrit Gosens, Tomas Kåberger, and Yufei Wang, "China's next renewable energy revolution: goals and mechanisms in the 13th Five Year Plan for energy," *Energy Science and Engineering* 5, no. 3 (June 26, 2017): 141-155, https://doi.org/10.1002/ese3.161.

14 As of 2019, China was producing about 7,112 terawatt-hours of energy per year, the U.S. about 4,461 terawatt-hours, and all of Europe about 4,077 terawatt-hours. "BP Statistical Review of World Energy," (London: BP, 2019), https://www.bp.com/en/global/corporate/energy-economics/statistical-review-of-world-energy.html.

15 "Global Energy Statistical Yearbook 2019," Enerdata, https://yearbook.enerdata.net/electricity/world-electricity-production-statistics.html.

16 2018 statistics from "2018 detailed electricity statistics" China Energy Portal, December 21, 2019, https://chinaenergyportal.org/en/2018-detailed-electricity-statistics-update-of-dec-2019/#.

17 "International Energy Outlook 2019 with projections to 2050," (Washington, DC: U.S. Energy Information Administration, September 2019), 103-104, https://www.eia.gov/outlooks/ieo/pdf/ieo2019.pdf.

18 The Economist Intelligence Group, "Regional China: Energy Structure," HSBC, August 13, 2018, https://www.business.hsbc.com/belt-and-road/regional-china-energy-structure; "Xinjiang sees steady growth in new energy power generation," Xinhua, July 28, 2019, http://www.xinhuanet.com/english/2019-07/28/c_138265256.htm.

19 Peter Fairley, "China's Ambitious Plan to Build the World's Biggest Supergrid," IEEE Spectrum, February 21, 2019, https://spectrum.ieee.org/energy/the-smarter-grid/chinas-ambitious-plan-to-build-the-worlds-biggest-supergrid.

20 "China's Arctic Policy" (Beijing: The State Council, The People's Republic of China, Jan 26, 2018), http://english.www.gov.cn/archive/white_paper/2018/01/26/content_281476026660336.htm.

21 Corrado Clini and Arvea Marieni, "China Plans UHV Transmission Lines that Span Continents," EnergyPost, March 22, 2019, https://energypost.eu/china-plans-uhv-transmission-lines-that-span-continents/.

22 The first official definition of Smart Grid was part of the 2007 Energy Independence and Security Act. Energy Independence and Security Act of 2007, Pub. L. No. 110-140 (2007), https://www.govinfo.gov/content/pkg/PLAW-110publ140/html/PLAW-110publ140.htm.

23 Laurie Chen, "China's Largest Utility Plans a National Power Grid Integrating Internet of Things Technologies," *South China Morning Post*, October 26, 2019, https://www.scmp.com/news/china/society/article/3034684/chinas-largest-utility-plans-national-power-grid-integrating.

24 "Opinions of the CPC Central Committee and the State Council on further deepening the reform of the electric power system (ZhongFa [2015] No. 9)," China Energy Portal, October 3, 2015, https://chinaenergyportal.org/en/opinions-of-the-cpc-central-committee-and-the-state-council-on-further-deepening-the-reform-of-the-electric-power-system-zhongfa-2015-no-9/.

25 Michael G. Pollitt, Chung-Han Yang, and Hao Chen, "Reforming the Chinese Electricity Supply Sector: Lessons from International Experience" (Cambridge, UK: Energy Policy Research Group, University of Cambridge, March 2017), https://www.energy.cam.ac.uk/news-and-events/news/reforming-the-chinese-electricity-supply-sector-lessons-from-international-experience.

26 Zhang Baoshu, "能源互联网：汇聚中国奋进的磅礴动力"[Energy Internet: Gathering the Power of China's Endeavor], Cyberspace Administration of China, August 15, 2018, http://www.cac.gov.cn/2018-08/15/c_1123271763.htm.

27 Wang Qi, Li Mengya, Tang Yi, and Ni Ming, "电力信息物理系统网络攻击与防御研究综述"[A Review of Research on Cyberattack and Defense in Cyber Physical Power Systems: Parts 1 and 2], 电力系统自动化 [*Automation of Electric Power Systems*] 43, no. 9, May 10, 2019, http://www.aeps-info.com/aeps/article/html/20180906006.

28 Rogier Creemers, Paul Triolo, Samm Sacks, Xiomeng Lu, and Graham Webster, "China's Cyberspace Authorities Set to Gain Clout in Reorganization," New America, March 26, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cyberspace-authorities-set-gain-clout-reorganization/.

29 Matt Sheehan, "How China's Massive AI Plan Actually Works," MacroPolo, February 12, 2018, https://macropolo.org/analysis/how-chinas-massive-ai-plan-actually-works/.

30 Lu Yingjia, "我国电力信息系统面临的网络安全风险及处置建议"[Network Security Risks Faced by China's Electric Power Information System and Suggestions], 中国信息安全 [China Information Security Magazine], December 31, 2019, https://www.secrss.com/articles/16328.

31 Ibid.

32 Ibid.

33 Ibid.

34 Ibid.

35 Ibid.

36 Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* (New York: Penguin, 2019), 14.

37 There are mentions of establishing separated, or air-gapped networks, but these are not highlighted as core technological solutions.

38 Elsa B. Kania and John K. Costello, "Quantum technologies, U.S.-China strategic competition, and future dynamics of cyber stability," 2017 International Conference on Cyber Conflict (CyCon U.S.), Washington, DC, November 2017, 89-96, https://ieeexplore.ieee.org/document/8167502.

39 Ibid.

40 Qiang Zhang, Feihu Xu, Li Li, Nai-Le Liu, Jian-Wei Pan, "Quantum Information Research in China," *Quantum Science and Technology* 4, no. 4 (November 8, 2019), https://iopscience.iop.org/article/10.1088/2058-9565/ab4bea/meta.

41 Stephen Chen, "Chinese Scientists Report Breakthrough on Quantum Internet Technology with Entangled Atoms," *South China Morning Post*, February 15, 2020, https://www.scmp.com/news/china/science/article/3050660/chinese-scientists-report-breakthrough-quantum-internet.

42 Immanuel Block, Harald Weinfurter, Hubert Filser and Martin Thurau, "Setting the Pace," Ludwig-Maximilians-Universität München, February 10, 2020, https://www.en.uni-muenchen.de/news/newsarchiv/2020/bloch_weinfurter_quantum.html.

43 Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo and Jian-Wei Pan, "Secure quantum key distribution with realistic devices," (Ithaca, NY: Cornell University, February 19, 2020), https://arxiv.org/abs/1903.09051v3.

44 Qiang Zhang, Feihu Xu, Li Li, Nai-Le Liu, and Jian-Wei Pan, "Quantum Information Research in China."

45 Yonghe Guo, "Application in Power Industry Promotes the Development of Quantum Cryptography Technology," (presentation, ITU Workshop on Quantum Information Technology for Networks, Shanghai, June 6, 2019), https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Pages/programme.aspx.

46 Mengmeng Xing, Guojun Liu, and Xu Lu, "Application of quantum secure communication technology in the power grid services," *Journal of Physics: Conference Series* 1303, The Second International Conference on Mechanical, Electric, and Industrial Engineering, Hangzhou, China (May 25-27, 2019), https://iopscience.iop.org/article/10.1088/1742-6596/1303/1/012087/meta.

47 Wang Yichen, "人工智能让电网变"聪明"了"[Artificial Intelligence makes the grid 'smart'], Cyberspace Administration of China, July 26, 2019, http://www.cac.gov.cn/2019-07/26/c_1124800367.htm.

48 Herman K. Trabish, "How does AI improve grid performance? No one fully understands and that's limiting its use," Utility Dive, November 14, 2019, https://www.utilitydive.com/news/how-does-ai-improve-grid-performance-no-one-fully-understands-and-thats-l/566997/.

49 Nektaria Kaloudi and Jingyue Li, "The AI-Based Cyber Threat Landscape: A Survey," *ACM Computing Surveys* 53, no. 1 (February 2020), https://dl.acm.org/doi/10.1145/3372823.

50 Ibid.

51 Y. Yang, J.Q. Ju, Q.H. Li, and Q. Wang, "An Experimental Research on Impacts of Malicious Attacks on PMU in Smart Grids," 2018 International Conference on Power System Technology (POWERCON), Guangzhou, China, November 6-8, 2018, https://ieeexplore.ieee.org/document/8602008.

52 Qi Wang, Wei Tai, Yi Tang, and Ming Ni, "Review of the false data injection attack against the cyber-physical power system," *IET Cyber-Physical Systems, Theory and Applications* 4, no. 2 (June 2019): 101-107, https://digital-library.theiet.org/content/journals/iet-cps/4/2.

53 Rongkuan Ma, Peng Cheng, Zhenyong Zhang, Wenwen Liu, Qingxian Wang, and Qiang Wei, "Stealthy Attack Against Redundant Controller Architecture of Industrial Cyber-Physical System," *IEEE Internet of Things Journal* 6, no. 6 (December 2019): 9783-9793, https://ieeexplore.ieee.org/document/8777097/.

54 Zang Yichao, Zhou Tianyang, Ge Xiaoyue, and Wang Qingxian, "An Improved Attack Path Discovery Algorithm Through Compact Graph Planning," *IEEE Access* 7 (May 17, 2019), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8708196.

55 Yi Han, Benjamin I.P. Rubinstein, Tamas Abraham, Tansu Alpcan, Olivier De Vel, Sarah Erfani, Davi Hubczenko, Christopher Leckie, and Paul Montague, "Reinforcement Learning for Autonomous Defence in Software-Defined Networking," (Ithaca, NY: Cornell University, August 17, 2018), https://arxiv.org/abs/1808.05770.

56 Cheng Lei, Hong-Qi Zhang, Jing-Lei Tan, Yu-Chen Zhang, and Xiao-Hu Liu, "Moving Target Defense Techniques: A Survey," *Hindawi* 2018 (July 22, 2018), https://new.hindawi.com/journals/scn/2018/3759626/.

57 "Secretary of the Navy Cybersecurity Readiness Review," (Arlington, VA: U.S. Department of the Navy, March 12, 2019), 6, https://www.navy.mil/submit/display.asp?story_id=108885.

58 "State of Threats to Electrical Entities in North America," Dragos, January 9, 2020, https://dragos.com/blog/industry-news/the-state-of-threats-to-electric-entities-in-north-america/.

59 Daniel R. Coats, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community," (Washington, DC: Office of the Director of National Intelligence, January 29, 2019), https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1947-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community. In the case of Russia, the U.S. has chosen to threaten their own power grid and make the activity public, see: David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *The New York Times*, June 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

60 "Senate Passes King Bill Protecting Energy Grid from Cyber-Attacks," Senator Angus King, June 28, 2019, https://www.king.senate.gov/newsroom/press-releases/senate-passes-king-bill-protecting-energy-grid-from-cyber-attacks.

61 "Summary, Department of Defense Cyber Strategy 2018," (Arlington, VA: U.S. Department of Defense, September 18, 2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

62 Ibid., 4

63 Ibid., 4

64 "Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command," (Fort Meade, MD: U.S. Cyber Command, April 2018), https://www.cybercom.mil/About/Mission-and-Vision/.

65 A very thorough accounting of the history of the strategy's development, as well as an analysis of the risks, is provided by Jason Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace," *Journal of Cybersecurity* 5, no. 1 (2019): 1-15. See also Herbert Lin and Amy Zegart, *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations* (Washington, DC: Brookings Institution Press, 2018).

66 "Summary, Department of Defense Cyber Strategy 2018," 5.

67 DCO-RA missions are normally actions taken in foreign cyberspace. "Cyberspace Operations," (Arlington, VA: Joint Chiefs of Staff, June 8, 2018), II-6, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150.

68 Daniel R. Coats, "Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community."

69 Scott W. Harold, Martin C. Libicki, and Astrid Stuth Cevallos, "Getting to Yes with China in Cyberspace," (Santa Monica, CA: RAND Corporation, 2016), 72-73, https://www.rand.org/pubs/research_reports/RR1335.html.

ABOUT THE AUTHOR

Tom Stefanick is a visiting fellow with the Security and Strategy team in the Foreign Policy program at the Brookings Institution. He is writing a book on impacts of artificial intelligence on the military to be published by Brookings Institution Press in 2020. From 1988 to 2018 he was a technical analyst and eventually a senior vice president at Metron, Inc., consulting mainly to the Navy. He led R&D efforts in machine learning, image recognition, lidar, autonomous planning, statistical modeling, sensor modeling, and computer simulation of naval operations. Prior to joining Metron in 1988, he was a science fellow in HASC working on Soviet submarine and strategic antisubmarine technology. Stefanick is the author of *Strategic Antisubmarine Warfare and Naval Strategy* (Lexington Books, 1987).

ACKNOWLEDGEMENTS

I would like to thank Michael O'Hanlon, Chris Meserole, Tarun Chhabra, Ted Reinert, and anonymous reviewers for substantive comments. Ted Reinert also edited this paper, and Rachel Slattery provided layout.