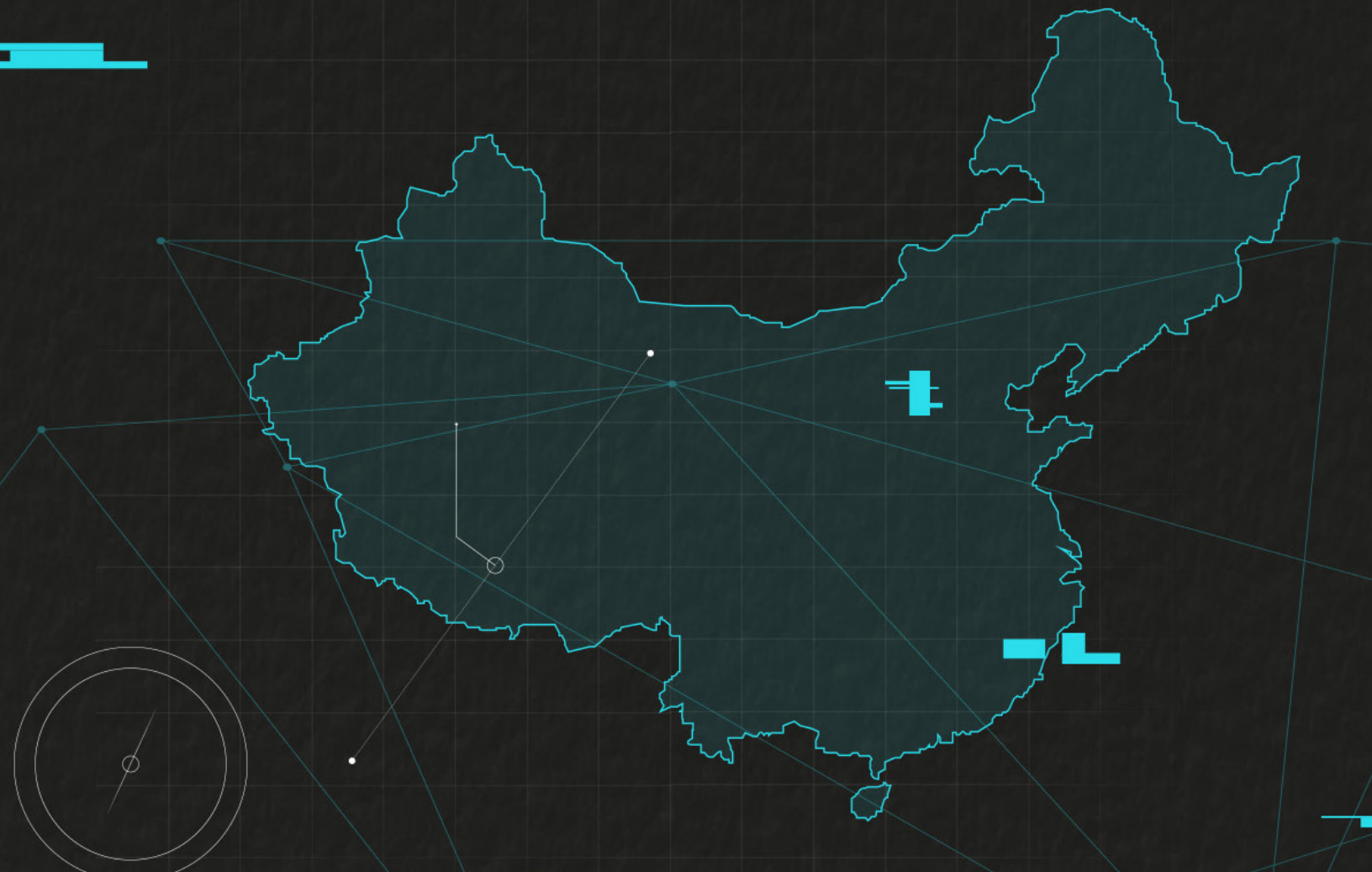
ARMIS®

THE STATE OF
CYBERWARFARE

WHITE PAPER

THE NEW WORLD ORDER IS SHAPED BY CYBERWARFARE CAPABILITIES OF EAST VS. WEST

CHINA



INTRODUCTION

Cyberwarfare is a growing concern for nations worldwide, and the offensive cyber capabilities of China and other nations hostile to Western interests are proving to be rapidly evolving. The issue of cyberwarfare has become even more pressing with multiple statements from the Department of Defense referencing 2025 as a potential year for a China altercation with Taiwan. This looming threat has led to the realization that any upcoming war between China and the rest of the world may be waged initially (and continually) in cyberspace and in lieu of kinetic warfare, with China's capabilities putting it at a significant advantage.

However, it's not just about China's cyber offensive capabilities. It's also about how much more vulnerable the West is compared to the east to disruption of our lifestyle.

Even simple things like disruption of internet or cellular service, or things like streaming services, can over time affect public opinion. Social media influence is a key weapon as well, where things like bank collapses can be exploited and amplified to cause further damage by swaying public opinion.

Cyberwarfare is an effective method of waging war, especially against western societies that have been so influential over the World order since the end of WWII. In recent years, China and others have developed extensive cyber espionage programs that target Western institutions in critical infrastructure, defense, and research. The Chinese government and others have invested heavily in building up capabilities, to wage cyberwarfare. Furthermore, China-affiliated "private" enterprises also play a key role.

The Chinese government, for example, is committed to building up its cyber capabilities and has made it a formidable force in the cyber domain. Similar to other hostile nations, China's cyberwarfare program is not limited to defensive measures but includes a broad range of offensive capabilities. These include sophisticated malware, zero-day exploits, and the ability to conduct Distributed Denial of Service (DDoS) attacks on a massive scale. The Chinese government has historically been known to engage in cyber espionage, stealing intellectual property and sensitive information from other nations.

This investment in offensive cyber capabilities is giving China a key weapon in its arsenal to exert their influence in the world order. It is no surprise that the Internet makes it easier (and cheaper) to wage cyberwarfare. In a conflict between hostile nations like China and the US, the cyber capabilities can be used to disrupt critical infrastructure, such as power grids and communication networks, effectively crippling the US or any Western nation's essential services; cyber warfare is

an incredibly useful, cheap, cost-effective tool of changing the world dynamics.

The threat of cyberwarfare on this scale has led to increased efforts by nations worldwide to enhance their own cyber capabilities. However, the fact remains that China and others continue to heavily invest in cyberwarfare capabilities. As a result, we are likely to see escalated use of cyberwarfare techniques on an accelerated scale never before seen in the coming few years.

In this kind of warfare, everyone is on the front line. Every company, every person. There are no borders. That's what makes this such an effective form of warfare. It's not just governments and militaries that need to be vigilant. Every business and individual has a role to play in protecting themselves and their assets from potential cyber-attacks.

The US and other nations are currently developing the defensive and offensive capabilities necessary to defend against cyber attacks. However, it is unlikely that any nation will be able to match China's capabilities anytime soon. The result is that we may see a significant shift in the way wars are fought, with cyber attacks becoming a primary weapon in conflicts between nations.

EAST VS. WEST: HOW DOES CHINA SEEK AN EDGE?

The Chinese government has been heavily investing in their cyber capabilities, with the country's defense budget increasing over the years. In 2020, China's defense budget was estimated to be around $178 billion, a significant increase from the previous year. This investment has enabled China to continue to build up its cyber capabilities, with the country having more than 50,000 cyber soldiers and an advanced cyber warfare unit.

The link between Chinese hackers and targeting security and networking appliances is a cause for concern, as it highlights the growing sophistication of cyber-attacks and the need for organizations to stay vigilant against such threats. By targeting security and networking appliances, hackers can gain access to sensitive information and critical systems, potentially causing significant damage to an organization's operations and reputation.

China's cyber espionage activities have been well documented, with the country being accused of stealing intellectual property and sensitive information from other countries. The Chinese government has also been linked to several high-profile cyber attacks, including the 2015 breach of the US Office of Personnel Management, which compromised the personal information of millions of US government employees.

The Chinese government's commitment to developing their cyber capabilities is not just limited to offensive measures but also includes defensive capabilities. China has been actively working on building up its cybersecurity infrastructure, which includes the development of new technologies such as artificial intelligence and blockchain to secure its networks.

The US continues to increase its efforts to counter the cyber capabilities of China and other hostile nations, with the government launching initiatives such as the National Cyber Strategy and the Cybersecurity and Infrastructure Security Agency (CISA). However, it is widely acknowledged that the US may be lagging behind China in terms of cyber capabilities.

The impact of cyberwarfare on critical infrastructure has been a growing concern for nations worldwide. In 2015, Ukraine's power grid was hit by a cyber attack, which caused a blackout that lasted for several hours. The incident highlighted the vulnerability of critical infrastructure to cyber attacks and demonstrated the potential impact that such attacks could have.

China's superior offensive cyber capabilities present a looming threat to the world, with the potential for cyber attacks to cause significant damage to critical infrastructure and disrupt economies. The development of defensive and offensive cyber capabilities has become increasingly important for nations to defend themselves against these attacks, and the US and other nations are currently engaged in a cyber arms race to develop these capabilities. However, with China's continued investment in its cyber capabilities, it is unlikely that any nation will be able to match its capabilities anytime soon. As such, the threat of cyberwarfare is likely to remain a significant concern for nations worldwide in the coming years.

THE GROWING CONCERNS OF CYBER ATTACKS ON CRITICAL INFRASTRUCTURE AND INTERNATIONAL RELATIONS

The potential for cyber attacks to disrupt economies and critical infrastructure is a growing concern for nations worldwide, particularly as more and more aspects of society become reliant on technology. One of the most significant concerns is the potential for cyber attacks to cause a blackout of power grids, which could have catastrophic consequences for society.

In addition to power grids, other critical infrastructure systems such as water treatment plants, transportation networks, and financial systems are also high value targets. Attacks on these systems could lead to significant disruption, with the potential for long-term economic and societal consequences.

The threat of cyber attacks is also significant in the context of international relations, particularly as tensions continue to rise between China and the US. In recent years, both countries have accused each other of engaging in cyber espionage and hacking, with the potential for cyber attacks to escalate into a full-blown cyber war.

The development of offensive and defensive cyber capabilities has become increasingly important for nations to defend themselves against these threats. However, the development of such capabilities is not without its ethical considerations, particularly in the context of the use of offensive cyber capabilities. The use of offensive cyber capabilities could potentially violate international law and lead to significant geopolitical consequences.

THE NEED FOR INCREASED CYBERSECURITY MEASURES AND INTERNATIONAL COLLABORATION TO ADDRESS CYBER THREATS

While China is widely recognized as one of the most significant threats to US cybersecurity, it is not the only country that poses a threat. Russia is also a significant player in the cyber warfare arena, having been accused of a range of cyber attacks on US targets, including the 2016 election interference.

Iran and North Korea are two other countries that are widely recognized as potential cyberwarfare threats to the US. Both countries have been accused of engaging in cyber attacks against US targets, with North Korea in particular being responsible for the 2014 cyber attack on Sony Pictures Entertainment.

Other countries, such as Israel, the UK, and France, are also developing advanced cyber capabilities, although they are generally considered to be more focused on defensive capabilities rather than offensive capabilities.

As the threat of cyber attacks continues to grow, the need for international cooperation in addressing the issue has become increasingly important. Many nations have taken steps to increase international collaboration on cyber security issues, such as through the establishment of information-sharing agreements and the development of international norms and standards.

However, the challenges of international cooperation on cyber security issues are significant, particularly in the context of geopolitical tensions between nations. As such, addressing the threat

of cyber attacks remains a significant challenge for nations worldwide, and one that is likely to remain a top priority in the coming years.

Managing the attack surface then is crucial. Organizations must be proactive in identifying and managing their assets, as they are the ones at risk of being attacked. It's not just about the technology used to protect these assets, but also about the people and processes involved in managing them. Every organization must be aware of the potential risks and have a plan in place to mitigate them.

In conclusion, the potential for cyberwarfare to cause significant damage to critical infrastructure and disrupt economies is a growing concern for nations worldwide. With China's superior offensive cyber capabilities, the threat of cyber attacks is particularly significant in the context of international relations. The development of defensive and offensive cyber capabilities has become increasingly important for nations to defend themselves against these threats, but the use of such capabilities raises ethical considerations and the potential for significant geopolitical consequences.

Having said that, other countries such as Russia, Iran, and North Korea also pose a significant threat. Developing advanced cyber capabilities has become increasingly important for nations to defend themselves against these threats, but international cooperation on cyber security issues remains a significant challenge.

As such, the threat of cyber attacks is likely to remain a top concern for nations worldwide in the coming years.

FURTHER READING

- THE ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT 2022-2023: https://www.armis.com/cyberwarfare/
- “China’s Cyber Power,” Center for Strategic and International Studies: https://www.csis.org/programs/technology-policy-program/chinas-cyber-power
- “China’s Cyber Capabilities,” Council on Foreign Relations: https://www.cfr.org/backgrounder/chinas-cyber-capabilities
- “U.S.-China relations: An overview of the current situation,” Council on Foreign Relations: https://www.cfr.org/backgrounder/us-china-relations-an-overview-of-the-current-situation
- “National Cyber Strategy,” The White House: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
- “Cybersecurity and Infrastructure Security Agency,” Department of Homeland Security: https://www.cisa.gov/
- “Ukraine Power Grid Hackers Probably Attacked U.S. Too, Experts Say,” Wired: https://www.wired.com/story/ukraine-power-grid-hackers-probably-attacked-us-too-experts-say/
- “Cybersecurity of the power grid: A growing challenge,” Brookings Institution: https://www.brookings.edu/blog/techtank/2019/05/02/cybersecurity-of-the-power-grid-a-growing-challenge/
- “The threat of cyber attacks on critical infrastructure,” World Economic Forum: https://www.weforum.org/agenda/2019/08/the-threat-of-cyber-attacks-on-critical-infrastructure/
- “The Ethics of Cyber Weapons,” Carnegie Endowment for International Peace: https://carnegieendowment.org/2017/03/20/ethics-of-cyber-weapons-pub-68224
- “Russia’s cyber capabilities,” Center for Strategic and International Studies: https://www.csis.org/programs/russian-studies-program/russias-cyber-capabilities
- “Iran’s Cyber Threats: Espionage, Sabotage, and Revenge,” Council on Foreign Relations: https://www.cfr.org/backgrounder/irans-cyber-threats-espionage-sabotage-and-revenge
- “North Korea’s cyber capabilities,” Council on Foreign Relations: https://www.cfr.org/backgrounder/north-koreas-cyber-capabilities
- “The Cyber Capabilities of Nations,” Global Security Review: https://globalsecurityreview.com/the-cyber-capabilities-of-nations/
- “International Cooperation on Cybersecurity,” The Cipher Brief: https://www.thecipherbrief.com/column/cyber-initiative/international-cooperation-cybersecurity
- “The Global Cybersecurity Landscape,” World Economic Forum: https://www.weforum.org/reports/the-global-cybersecurity-landscape-2019

THE STATE OF
CYBERWARFARE

ABOUT ARMIS

Armis, the leading asset visibility and security company, provides the industry's first unified asset intelligence platform designed to address the new extended attack surface that connected assets create. Fortune 100 companies trust our real-time and continuous protection to see with full context all managed, unmanaged assets across IT, cloud, IoT devices, medical devices (IoMT), operational technology (OT), industrial control systems (ICS), and 5G. Armis provides passive cyber asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in California.

armis.com

info@armis.com

20230110-1

ARMIS®