

# (U) U.S. and China: Comparison of Cyber Capabilities

(U) by: Christopher Hekimian

## Contents

(U) Executive Summary .....	5
1.0 (U) Introduction .....	7
1.1 (U) Methodology .....	7
2.0 (U) Overarching Contrasts in Principles Guiding China and U.S. in Cyberspace .....	8
2.1 (U) Risks posed by Cyber Warfare.....	8
2.2 (U) Evolution of Chinese Cyber Capabilities.....	8
2.3 (U) Cultural Differences Impacting the Flow of Information in China .....	9
2.4 (U) Contrasts on what Constitutes “Cyberspace” and “Cyber Warfare” .....	9
2.5 (U) Divergent Norms of Behavior in Cyberspace .....	10
2.6 (U) Informationalized Warfare.....	10
2.7 (U) Integrated “Whole of Government” Approach to Warfare .....	11
2.8 (U) Objectives of China’s Offensive Cyber Operations (OCOs) .....	12
2.9 (U) Attribution and Diverse Approaches to Cyber-Policing .....	13
3.0 (U) Contrast in Cyber R&D in China and U.S. ....	14
3.1 (U) Chinese Interest in National Surveillance .....	14
3.2 (U) Cybersecurity Recruitment Efforts.....	14
3.3 (U) The Differing Perception of Hackers in China and U.S. ....	15
3.4 (U) The Tianfu Cup .....	15
3.5 (U) Mandatory Disclosures of Software Vulnerabilities.....	16
3.6 (U) Chinese Industry and Cyber Research.....	17
3.7 (U) Military and Academia Coordination on Cyber Research .....	17
3.8 (U) R&D Dependency on Materiel Supply Chains .....	19
3.9 (U) Diverse Norms of Behavior Impacts to Cyber R&D .....	20
3.10 (U) R&D Capability for Cyberwar Involving Complex Infrastructure Targets .....	20
3.11 (U) R&D Focus on Artificial Intelligence and Machine Learning (AI/ML) .....	21
3.12 (U) R&D Focus Quantum Applications .....	21
4.0 (U) Technology Insertion in China and U.S. ....	22
4.1 (U) Contrast in Cyber Acquisition Processes .....	22
4.2 (U) Civilian-Enabled Technology Insertion .....	23

4.3 (U) Domestic Industry-Enabled Technology Insertion .....	24
4.4 (U) Foreign-Enabled Technology Insertion .....	24
4.5 (U) University-Enabled Technology Insertion .....	24
4.6 (U) Chinese Ability to Insert Technologies Rapidly .....	25
4.7 (U) U.S. Cyber Technology Insertion Time .....	25
5.0 (U) Operational Effectiveness .....	26
5.1 (U) Bases for Distinction of Operational Effectiveness .....	26
5.2 (U) Defining Offensive Cyber Operations.....	27
5.3 (U) Attribution.....	27
5.4 (U) Strategic Approach: Network Warfare.....	29
5.5 (U) Strategic Approach: Cyber Force Size .....	30
5.6 (U) Strategic Approach: Concurrent Criminal Operations .....	31
5.7 (U) Strategic Approach: Characteristically Active .....	31
5.8 (U) Strategic Approach: Cyber Espionage .....	33
5.9 (U) Strategic Approach: Infrastructure as a Target.....	34
5.10 (U) Strategic Approach: Leveraging International Cooperation .....	34
5.11 (U) Strategic Approach: Norms of Behavior.....	35
5.12 (U) Enabler: Cyber- Enabling Laws .....	35
5.13 (U) Enabler: Domestic Surveillance.....	36
5.14 (U) Enabler: Drawing on Civilian Institutions .....	37
5.15 (U) Enabler: Drawing on Civilian IT Infrastructure .....	38
5.16 (U) TTP: Cyber in Context with Gray-Zone Tactics .....	38
5.17 (U) TTP: OCOs as Elements of Complex Attacks .....	40
5.18 (U) TTP: Vulnerability Mining .....	41
5.19 (U) TTP: Leveraging Civilian Computers .....	42
5.20 (U) TTP: Supply Chain Attacks .....	42
5.21 (U) Comparative Assessments in OCOs .....	43
5.22 (U) Conclusions .....	47
6.0 (U) Relative Abilities to Counter Cyber Threats .....	49
6.1 (U) Cyber Connectedness and Dependencies.....	50
6.2 (U) Cyber Freedom and Information Controls .....	50
6.3 (U) Attributes of Current Cyber Threats .....	51
6.4 (U) Cyber Vulnerabilities .....	52

6.5 (U) Contrasting DCO Approaches.....	53
6.6 (U) Defending Against “Botnets” .....	55
6.7 (U) Cybersecurity System Patches .....	55
6.8 (U) Defensive Cybersecurity Posture and Priority .....	56
6.9 (U) Conclusions .....	58
7.0 (U) Recommendations to Improve the Cybersecurity Posture of the U.S.....	60
7.1 (U) Continue to Emphasize Zero-Trust Architectures and Multi-Factor Authentication.....	60
7.2 (U) Raising Awareness and Improving Cybersecurity Education .....	60
7.3 (U) Survey Chinese-sourced Network Technology and Perform a Risk Assessments.....	61
7.4 (U) Engagement with Domestic Hacker Community .....	61
7.5 (U) Make Optimal Use of the Department of Commerce Entity List .....	61
7.6 (U) Pre-emptively Engage with Wider International Audience on Cybersecurity .....	61
7.7 (U) Improve Domestic Vulnerability Detection Process .....	61
7.8 (U) Enhance Code Supply Chain Security .....	62
7.9 (U) Make a Cybersecurity Common Operational Picture Available to Wider U.S. Cybersecurity Stakeholder Community. ....	62
7.10 (U) Enable Some Private Sector OCO’s and DCO’s.....	62
7.11 (U) Emphasize Cyber S&T Efforts that would leverage AI .....	62
7.12 (U) Move Toward Closed IT Standards for Critical Applications .....	62
7.13 (U) Improve Communication on OCO Justification .....	63
7.14 (U) Build Trust and Earn Back Cyber-Credibility .....	63
(U) Acronyms .....	63
(U) References.....	66

This page intentionally left blank

## (U) Executive Summary

(U) Section 1251 of the fiscal year 2022 National Defense Authorization Act (FY22 NDAA) directed the OUSD(R&E), by modernization area, to conduct comparative studies that would compare the U.S. capabilities with those of the People's Republic of China (PRC). This document is the result of the comparative capabilities study based on unclassified or open-source information supporting the cyber modernization area. The format of this document is aligned with the general requirements specified in Section 1251.

(U) The main sections of the document were based primarily on section 1251 requirements and are:

1. Introduction  
The introduction section describes the genesis of the report starting with the 2022 NDAA Section 1251 requirements and the general methodology followed in the development of the document.
2. Overarching Contrasts in Principles Guiding China and U.S. in Cyberspace  
This section introduces and highlights some of the distinguishing social, political and cultural features that impact the cybersecurity postures and strategies of the Peoples Republic of China (PRC) and the U.S. The section introduces the theme that the social, political and cultural parameters behind the cybersecurity strategies and national objectives for both countries are very different. One almost needs to abandon a western and Anglo-centric perspective in order to view the PRC objectives, especially as they apply to cybersecurity and informationalized warfare in context.
3. Contrast in Cyber Research and Development (R&D) in China and U.S.  
This section describes the different approaches to supporting R&D and the industrial base supporting cybersecurity in each country. Overarching national objectives and prioritizations at the highest level of government become evident in the contrasting approaches.
4. Technology Insertion in China and U.S.  
This section reflects the theme that the command economy of the PRC is particularly well-suited for technology insertion in support of Chinese Communist Party (CCP) objectives. This is especially true when compared with the overall defense acquisition process embraced by the U.S. which is rarely described as efficient.
5. Offensive Operational Effectiveness  
This section highlights factors that tend to improve the offensive operational effectiveness of the PRC asymmetrically in that respect for international law, ethics, decency and personal freedoms would preclude the U.S. from exploiting the same methods at a comparable scale. Imposition of a surveillance state, militarization of industry and academia figure prominently in the CCPs ability to conduct large-scale cyberwarfare against a wide range of targets. Cyberespionage and the willingness of the People's Liberation Army (PLA) and Ministry of State Security (MSS) to turn blind eye

towards criminal activities carried out by their cyberwarrior proxies comes with operational advantages that are not and should not be enjoyed by the U.S..

6. Relative Abilities to Counter Cyber Threats

A major theme in this section is that the elements that contribute to a robust or large-scale offensive cyber capability will tend to contribute to a robust defensive capability. Also, the surfaces of vulnerability characteristic of the PRC and the U.S. are very different with the Chinese enjoying the reduced surface. Elements of societal “connectedness” and the effects of censorship and surveillance all contribute to a reduced surface of vulnerability for the PRC. The importance of an educated public and improved communication about the threat and realities of cyberwarfare figure prominently as a necessary avenue for U.S. cyber defensive improvement.

7. Recommendations to Improve the Cybersecurity Posture of the U.S.

This section presents some recommendations found in the literature and from the research team.

## 1.0 (U) Introduction

(U) Section 1251 of the fiscal year 2022 National Defense Authorization Act (FY22 NDAA) directed the OUSD(R&E), by modernization area, to conduct comparative studies that would compare the U.S. capabilities with those of the People's Republic of China (PRC). Section 1251 clearly specifies the minimum requirements for the study.

(U) This document is the result of the comparative capabilities study based on unclassified or open-source information supporting the cyber modernization area. The format of this document is aligned with the general requirements specified in Section 1251.

### 1.1 (U) Methodology

(U) The study is based on three parallel literature review efforts focusing on open-source and unclassified materials (i.e., this document) and classified appendices based on sources available on SIPR<sup>1</sup> and JWICS, respectively. Each effort would identify and include information to support the Section 1251 requirements.

(U) Organization of this document is based on the requirements specified in Section 1251 and includes the following sections:

- Overarching Contrasts in Principles Guiding China and U.S. in the Cyber Realm
- Chinese/ American Cyber Research and Development (R&D) Efforts
- Relative Abilities to Transition and Insert Technologies
- Comparison of Operational Effectiveness between Chinese and American Cyber Operations
- Comparative Abilities to Counter Cyber Threats
- Recommendations

(U) More than 210 unclassified sources were explored during the course of developing this document.

---

<sup>1</sup> On 9/11/2023 an enterprise search was done on the intelshare resource on SIPR. A search all web-accessible documents dated between 1/1/2019 and 9/11/2023 that had the terms "China" and "Cyber" in the titles and which did not reference (U-KWT) in the title, yielded 248 results. The first 40 of the returned hits were examined and were found to be FBI Tearline-type reports of no use to the current study. The FBI tearline reports describe the technical details of specific cyber incidents. Further prosecution of the SIPR network for the study was halted due to the low likelihood that information relevant to the current study, especially articles and reports from commercial cybersecurity specialists that wouldn't be found in unclassified sources, would be found on SIPR.

## 2.0 (U) Overarching Contrasts in Principles Guiding China and U.S. in Cyberspace

(U) The following section highlights some areas of contrast between the Chinese and U.S. societies and cultures that influence strategic thinking about cyberspace and cyber superiority.

### 2.1 (U) Risks posed by Cyber Warfare

(U) Cyber effects can have devastating and deadly impacts against a victim nation. Particularly a technologically advanced (read: "dependent") nation like the United States of America.

Cyberattacks have the potential to paralyze food production and distribution; policing; make personal wealth disappear; paralyze the financial system; halt industry; turn the lights out on our power grid; cut-off our means to communicate and paralyze our water supply and our sanitation services. These effects are analogous to those created by a nuclear attack- except without the radiation and stigma associated with the escalation of conflict to the nuclear level. <sup>1</sup>

(U) The 2021 Chinese People's Liberation Army (PLA) article entitled "Analysis of Strategies for Interactions in Cybersecurity" observed, "From a cost-benefit point of view, attacks on key national critical infrastructure [defined as electrical and water, transportation, communications, air, and nuclear power] and military targets can be most effective, and they are the best choice for coercing the target country through cyberattacks." <sup>2</sup> Senior PLA colonel and researcher at the Nanjing Command College Cao Zhengrong, set forth in 2006 that network attacks could paralyze a nation's economy, sow societal disorder and allow one country to impose its will upon another- and that it could be done in times of peace or during war. <sup>3</sup>

(U) In terms of proof that the PRC is not above blatant acts of sabotage against the digital infrastructure of their adversaries, In February, 2023 boats flying Chinese flags severed submarine internet cables connecting the Matsu Islands from greater Taiwan. The attack on the cables had the expected effect of isolating the islands digitally and severely restricting commerce and banking. <sup>4</sup>

(U) The Chinese are aware that these kinds of effects will likely cause widespread fear, panic and lawlessness as people struggle to meet the everyday requirements of food, water and shelter. Hence, cyber and other gray zone tactics could be used to destabilize the U.S. and weaken the resolve of its people. Potentially, the PRC and the Chinese Communist Party (CCP) that rules it, would meet its primary military objective of ruling over the United States without ever having to fire a single gunshot.

(U) Review of the literature resulted in some sources claiming that the CCP is seeking cyber-parity with the United States. This analyst suggests that a review of the literature clearly indicates that the CCP is not interested in parity, but rather dominant superiority.

### 2.2 (U) Evolution of Chinese Cyber Capabilities

(U) The July 2021 indictment against four Chinese cyber threat actors states that hacks that used to be conducted using "sloppily worded" spearfishing emails by the PLA are now carried out by an "elite satellite network of contractors at front companies and universities that work at the



direction of China's Ministry of State Security (MSS).<sup>5</sup> From that state, China's cyber superiority initiatives have quickly propelled it to become the dominant cyber threat facing the United States. Tom Hegel, a senior threat researcher at cybersecurity intelligence firm SentinelOne indicated that China "stands out as the leading nation in terms of threat relevance, at least for America." <sup>6</sup> Marc Burnard, a researcher at Secureworks, observed "It's quite difficult to point out what the key (targeted) sectors are for China, because they target so many," Burnard said. "It's a scale that just completely dwarfs anything from the likes of Iran, North Korea and Russia." <sup>7</sup>

### 2.3 (U) Cultural Differences Impacting the Flow of Information in China

(U) Unlike the relative openness of western cultures to the flow of information, especially within cyberspace, the Chinese see the internet, as an information delivery system that must be controlled. Means include real-time censorship and technical control over the internet within China. The belief that information must be controlled led to implementation of the Great Firewall of China, which monitors all traffic in Chinese cyberspace and enables Chinese authorities to deny access to selected websites or even to disconnect all Chinese networks from the global internet. Thus, the Chinese and the U.S. tend to view cyberspace as a national resource, very differently. The Chinese historically understand that information as the key to victory.<sup>8</sup>

(U) In contrast with western societies where political parties are in theory, subordinate to the government, in China, the CCP is the ultimate authority over the PLA and the MSS, (the Chinese Intelligence Service) and all of China's economic and infrastructure entities. The CCP is able to draw upon the resources of China's enterprises and the PLA and MSS report directly to the CCP's Central Military Commission.<sup>9</sup>

(U) As a political party, the CCP has objectives that go beyond what would be considered traditional military ones. The CCP controlling the flow of information to and from the population would not be considered a military objective in the U.S. but in China doing so is considered vital to the CCP's ability to maintain control over the population and its political power.<sup>10</sup>

### 2.4 (U) Contrasts on what Constitutes "Cyberspace" and "Cyber Warfare"

(U) The United States views cyberspace as its own domain of potential conflict. In contrast, China considers cyberspace an enabler within a broader, information domain that emphasizes the control of information.<sup>11</sup> Another fundamental area of divergence between the U.S. and China on matters related to cyber is that China doesn't rely on the term "cyber" to the extent that the West does. To China, the concept of "informationalization" is the dominant term. Informationalized warfare is a concept that merges cyber warfare and information warfare. That they consider "cyber concepts" – in the West as tools and components of broader, information warfare-enhanced operations demonstrates a strategically nuanced view and one that impacts the way they employ cyber operations and the objectives and scope of those operations.

(U) Admiral Michael Rogers, the former Director of the National Security Agency (NSA DIR) points out a fundamental contrast in how cyber operations are viewed by the U.S. and by China. The Chinese view cyber as a tool to generate economic advantages over their adversaries. Their applications of cyber go well beyond what the United States would consider for national security

purposes.<sup>12</sup> There is no evidence that the U.S. government is carrying out offensive cyber operations (OCO) against China or any other country to exact any kind of economic gain.

(U) PRC President and Chairman of the CCP, Xi Jinping views cyberspace as an arena of fierce strategic competition that China must shape in its favor. He has stated that a country's ability to master the internet determines its rise or fall and that "those who win the internet win the world." He also expressed that "without cybersecurity there is no national security."<sup>13</sup> It's not clear whether U.S. leadership attribute the same degree of critical importance towards cyber dominance as the PRC leadership does.

## 2.5 (U) Divergent Norms of Behavior in Cyberspace

(U) The U.S. remains frustrated that the Chinese refuse to acknowledge the cyberattacks that the U.S. has attributed to them based on collected evidence. As a result, the U.S. perceives the Chinese as lawless in the cyber domain. The Chinese on the other hand, perceive U.S. efforts to force an admission of culpability as an attempt to force China to accept U.S. hegemony in the cyber domain.<sup>14</sup> Dean Cheng, a former senior research fellow in Asian studies for the Heritage Foundation cited China's repeated and enduring incursions into Indian territory in 2021 as an example of how Chinese thought on crisis stability and risk differs from that of the United States. Chinese leadership understands the reluctance of countries with lesser armed forces, population and nuclear arsenals to enter into an escalation match with the PRC and the PRC exploits that.<sup>15</sup>

(U) There are reports in the literature about OCOs being waged by the U.S. against its adversaries in the context of intelligence operations or in pursuit of military objectives. While the U.S. declines to self-attribute on these cases, a distinction can be made between the large scale OCO campaigns – packaged with cyber-crime payloads- waged against the U.S. by the Chinese and the more surgical and infrequent OCOs waged by the U.S.

(U) It is notable that the concept of attribution of OCOs is more relevant to the U.S. that is under some degree of public and moral pressure to respond to attacks in a targeted and proportional way. Attribution is likely less important to offensive cyber actors like the PRC, that are usually in a position of cyber-belligerence.

## 2.6 (U) Informationalized Warfare

(U) A key distinction between how the Chinese strategize against the U.S. in terms of cyber warfare involves the concept of "Informationalized Warfare". Informationalized warfare involves the direct targeting of civilians with fear, misinformation, threats and demoralization. Informationalized warfare, including intelligence, technical reconnaissance, cyber warfare, and electronic warfare, are central to China's strategies for asymmetric warfare and pre-emptive attack. China's ongoing military reforms that support a 'combined wartime and peacetime military footing', can be expected to give China an advantage should war break out against the U.S.

(U) Dominance in the information space enabled through network warfare (i.e., cyber) would enable paralyzing attacks against U.S. operational and command systems impacting all other domains: air, sea, land and space.<sup>16</sup> Information dominance would also serve to galvanize

support for war efforts within the Chinese population as well as undermining the same kind of support in the U.S.. It could also predictably erode morale and confidence within the U.S. through attacks on infrastructure, financial networks, supply chains, and on a broad range of American institutions.

(U) In 2000, a PLA strategist wrote in a Chinese National Defense University (NDU) textbook of the potential for "sending a message to the enemy" through an attack on their computer networks and precipitating the enemy to give up without a fight.<sup>17</sup> Perhaps a report by Nissen et al expresses the key point most succinctly when it states "We live in an asymmetric era in which dominance is won through non-kinetic exploitation of open societies."<sup>18</sup>

(U) There are no indications in the unclassified literature about U.S. efforts to target the Chinese population en masse with messaging intended to instill fear, mistrust and uncertainty. Nor would any such messaging be likely to penetrate the Chinese firewall of censors if such a campaign did exist. Therefore, in the context of the China/U.S. rivalry, the concept of informationalized warfare tends to be asymmetrically applied by China.

## 2.7 (U) Integrated "Whole of Government" Approach to Warfare

(U) Consistent with the concept of informationalized warfare and demonstrated by military operations other than war (MOOTW) or "grey-zone tactics", China has been observed to prefer integrated operations that at once, distract, destabilize, generate political pressure, strain the alliances of their adversaries, induce economic strain and demoralize populations.<sup>19</sup> Contrasting informationalized warfare support structures in China and U.S., Avril Haines, the Director of National Intelligence, testified before Congress in March of 2022 that "China is especially effective at bringing together a coordinated whole of government approach to demonstrate its strength and to compel neighbors to acquiesce to its preferences...".<sup>20</sup> The whole of government approach is comprised of elements of information warfare, psychological warfare, network warfare, intelligence operations and political and economic pressure. No one of these tactics rises to the level of warfare by itself, but the combined effect of them can be devastating- especially when cloaked in some degree of plausible deniability. Over time, victim countries tend to acquiesce to higher levels of economic, administrative, and cultural subversion. The victim populations in western cultures are subject to diverse messaging- including from sources influenced by China- and are reliably unsure of where malign outside influence ends and where ill fortune begins.

(U) The CCP's Strategic Support Force (SSF), under the PLA, brings together China's electronic warfare, network warfare (including cyber), space forces, information warfare and psychological warfare capabilities. This hybridized force approach is not apparent in the U.S., where the same capabilities would span as many as four separate commands and even agencies outside of the realm of the U.S. military.<sup>21</sup> The Chinese MSS also has keenly developed cyber capabilities but they also have intelligence collection and management functions that work to compromise humans that are in positions to be managed and exploited to achieve strategic or tactical advantages in cyberspace.<sup>22</sup>

(U) The one-party state of China under control of the CCP is uniquely suited for an integrated whole of government approach to warfare. Westernized countries with viable multi-party systems are typically not as well-suited. In the case of the United States, it is rare to see any kind of solidarity of purpose among elected representatives.

## 2.8 (U) Objectives of China's Offensive Cyber Operations (OCOs)

(U) Asia expert Nathan Beauchamp-Mustafaga identified one of the overarching objectives for Chinese OCOs as undermining an enemy's will to fight. One of the themes presented in the book entitled "Long-Distance Operations", an influential Chinese military strategy book published in the 1990's is "the need to target an adversary's homeland and bring the threat to an enemy's civilian population." the author of that book, Jiang Yamin, was a senior colonel in the PLA but was later promoted to major general and placed in charge of the Chinese military academy's Combat Theory and Regulations Research Department.<sup>23</sup>

(U) Beauchamp-Mustafaga et al, also identified an objective as "reducing an adversary's potential to conduct war."<sup>24</sup> This analyst would add that the Chinese also use OCOs to steal intellectual property in order to gain economic advantages and to overcome technical capability gaps. The PRC has also employed OCOs in an intelligence support role where targeted individuals can be identified for further development into intelligence assets or otherwise compromised.

(U) The Chinese view cyber as a strategic domain and a critical component of its overall deterrence strategy.<sup>25</sup> In 2009 a PLA textbook observed that cyber operations, including information operations (IOs), could "sow fear and panic amongst the enemy" and "compel adversaries away from rash activities."<sup>26</sup>

(U) In the U.S. it is not typical that our industry publicizes the successful cyberattacks waged against them or even their successful efforts of defending against those attacks. Most Americans are unaware of the ongoing conflicts in cyberspace that their banks, online merchants and government entities are engaged in on a continuous basis in order to safeguard information, wealth and to maintain operations. Publicizing the extent of cyber risks to the general public would be perceived as being "bad for business". Americans want to feel that their information, wealth and property are secure. For decision makers in the U.S. government, however, a simple example demonstrates the potential of OCO's to impact decision making on national security issues at the highest levels. Imagine the deterrent effect that shutting down the DoD Information Network (DODIN) even for a few hours, and in a few selected zones would have on high-ranking American political decision makers. If a cyber aggressor can demonstrate an ability to "shut out the lights" in the seat of its adversary's military planning and administration capability, the message that would convey about the potential to wage a successful resistance campaign should not be underestimated. Once again, citizens might not be made aware of such actions- nor are they likely to be targets of that kind of deterrent message, but that kind of deterrent in the hands of the Chinese is very valuable.

UNCLASSIFIED

(U) There was no indication in the unclassified literature that the U.S. engages in large scale cyber espionage for economic benefit or that there is a desire on behalf of the U.S. to sow fear and discord among the Chinese population as a matter of policy.

(U) To reinforce the notion that the fictional example given above is reasonable, on 25 May 2023 the Carlos Del Toro, the Secretary of the Navy, disclosed that Chinese hackers had infiltrated Navy infrastructure by a cyberattack and that such attacks were common. Microsoft Corporation indicated that the attack occurred against the territory of Guam.<sup>27</sup>

## 2.9 (U) Attribution and Diverse Approaches to Cyber-Policing

(U) According to a 2016 report by RAND, the U.S. feels that it can accurately attribute cyberattacks waged by the PRC to the PRC. Additionally, the report states that the U.S. seeks a means to exact some form of internationally-backed punishment against the PRC for those acts of aggression. In contrast, the report contends that the PRC does not believe that it can accurately assign attribution to U.S. attacks and so it opposes any internationally applied measures that would rely on any such attribution.<sup>28</sup> Elements of the CCP will issue public statements condemning the U.S. for cyber transgressions that it is able to attribute to the U.S.. However, there is no indication that they support empowering any sort of international cyber police or authoritative office that isn't under its direct control.

### 3.0 (U) Contrast in Cyber R&D in China and U.S.

(U) Nation states and the contractors they use aren't typically forthcoming with details about their cyber related research and development initiatives. Consequently, this section will focus on some indicators from which inferences can be made. The section will not address individual research initiatives underway by either country. Very little information of that kind is available on Chinese cyber R&D initiatives. Without full information for both sides, this section will focus solely on comparative cyber R&D related themes and known, R&D enablers.

#### 3.1 (U) Chinese Interest in National Surveillance

(U) Chinese interest in national surveillance has led to a multitude of small to large companies answering PLA requirements for cyber-related surveillance products of the PLA. As a result, the PRC has a portion of its cyber industry dedicated to identifying vulnerabilities in products like iPhone, Android and other platforms in widespread use in the western world. The number of zero-day vulnerabilities identified against these platforms is measured in the hundreds. China's appetite for surveillance and cyber technologies has resulted in a Chinese domestic ecosystem of small to large companies- including startups- that the PLA uses to conduct cyber operations and to meet PLA objectives in the cyber domain.<sup>29</sup> The demand posed by the PLA has also resulted in the migration of some cybersecurity firms from outside the PRC to the PRC. Qihoo 360, and Megvii are examples of companies specializing in cloud security, data security, zero trust and privacy relocating to the PRC to meet PLA requirements.<sup>30</sup>

(U) The Chinese domestic surveillance program has led to an important cyber R&D resource that is not available to U.S. researchers. As the Chinese advance their "Smart Cities" initiative as part of their effort to conduct broad scope surveillance on their population, they are also building digital twins of the cities. The digital twin technology is integrated with the Smart Cities to provide user interface features for monitoring systems and for command and control.<sup>31</sup> The digital cities would provide a fertile testbed for studying the ramifications of multiple, coordinated cyber-attacks on infrastructure assets and would provide a meaningful research- bed for planning large-scale OCO and DCO concepts.

(U) American interest in centralized surveillance of the population doesn't appear to match the scale of the domestic surveillance effort carried out by the CCP. The investment in surveillance technology, personnel and infrastructure infuses investment into cyber-related research.

#### 3.2 (U) Cybersecurity Recruitment Efforts

(U) The 2022 Global Threat report by CrowdStrike indicated that cyber security teams in the U.S. were strained in 2021 and that there is an ongoing cybersecurity skills shortage.<sup>32</sup> There are no indications in the literature that the PRC is experiencing a similar shortage of cyber professionals. The PRC's cybersecurity recruitment efforts included the "Thousand Talents" Plan that provided incentives for Chinese cyber researchers and professionals outside of the PRC to return to the PRC - to reverse what it perceived as a "brain drain of vital cyber talent."<sup>33</sup> A CrowdStrike intelligence report identified a recruitment campaign for the SSF of the PLA. The recruiting campaign was directed toward "English and Russian speaking linguists, and technical



experts in cybersecurity, artificial intelligence, pattern recognition, big data, geographic information systems (GIS), signal processing and foreign military capabilities." <sup>34</sup>

The U.S. is addressing the issue of cybersecurity “brain drain” a different way which is characterized in the DoD cyber workforce strategy released in March 2023. In this strategy DoD passively accepts the trend towards attrition of DoD trained cybersecurity experts to industry in anticipation of a large number of highly skilled cybersecurity professionals defending the nations cyber assets from the industry perspective. Mark Gorak, the principal director for resources and analysis for the DOD Chief Information Officer suggested that enduring relationships with former DoD cybersecurity professionals that have accepted positions in industry could be drawn upon in times of national need for one to three months as part of an informal partnership of sorts.<sup>35</sup>

To contrast the two approaches for attracting, retaining and developing a world class cybersecurity force, the PRC is aggressively attempting to attract talent back to the PRC’s cyber forces with incentive programs. The U.S. DoD is accepting a role as a training ground for industry cybersecurity professionals in the hopes that their work for industry will have a meaningful effect in support of the nations cybersecurity and that they will be available to volunteer their skills in times of national emergency.

The U.S. DoD also promotes its “Hacking for Defense” (H4D) initiative in concert with members of the intelligence community (IC). The H4D initiative allows participating college students insights into the broad range of challenges faced by DOD and the IC. Then, the students work on prototypes to address the challenges.<sup>36</sup> Unlike what the name suggests, H4D is not focused on cybersecurity issues and its scope includes a large range of technical challenges associated with national security. As such, it is a meaningful way to cultivate talent and attract young people to defense-related technical fields.

### 3.3 (U) The Differing Perception of Hackers in China and U.S.

(U) J.D. Work, senior fellow with the Atlantic Council’s Cyber Statecraft Initiative and professor at the National Defense University’s College of Information and Cyberspace notes a distinct difference between how Chinese and western hackers perceive their governments and the corporations whose products they seek to exploit. In the PRC, the government tends to understand and support the activity of hackers- who are often misunderstood. The hackers perceive themselves as assets vital to national security. In contrast, any positive government overtures from the West to its own hacker community are muted if they exist at all. And hackers tend to have an adversarial relationship characterized by mistrust with the western governments and with industry.<sup>37</sup>

### 3.4 (U) The Tianfu Cup

(U) The Tianfu cup cybersecurity “hacker” competition was an example of the CCP weaponizing sharp young minds in the PRC and filling them with a sense of purpose. <sup>38</sup> According to the Tianfu Cup webpage for the 2022 competition, the Tianfu Cup is intended to "build the most professional international cyber security event in southwest China and promote the high-quality development of China's cyber security industry." <sup>39</sup> The Tianfu Cup was essentially a

competition comprised mainly of patriotic Chinese trying to find and exploit vulnerabilities in prominent western communication and networking products. The Tianfu Cup served as a cyber "Show of Force" for the CCP and it demonstrated the high level of commitment on behalf of the CCP to OCOs and the industrial base in the PRC that supports them.<sup>40</sup> It also had the effect of reinforcing the notion that the U.S. (and the West) had a smaller pool of cyber talent than the PRC.<sup>41</sup>

(U) In 2021 the Tianfu Cup organizers distributed \$1.88 M in prizes to hackers who uncovered new vulnerabilities in Windows 10, Google Chrome, iOS 15, Apple Safari to Microsoft Exchange Server, Linux, and Ubuntu 20.<sup>42</sup> The Tianfu Cup sponsors included prominent firms within the Chinese defense industrial base and there are rumors of linkages to the Chinese Ministry of State Security.<sup>43</sup>

(U) The CCP restricts Chinese cybersecurity experts from participating in international challenges like Tianfu Cup outside of China because such events tend to disclose vulnerabilities too publicly such that they could be patched before they could be exploited by the CCP.<sup>44</sup> Would-be participants must receive permission from the government and that permission is rarely granted.<sup>45</sup>

(U) Chinese-backed competitions like the Tianfu Cup and more importantly- the mindset that cultivates generations of skillful and determined hacker forces position the Chinese at an advantage over the U.S. in terms of research to find new vulnerabilities and in terms of locating and grooming new cyber researchers.

(U) While international hacking competitions exist elsewhere (such as the Pwn2Own events held in Canada) cyber intelligence expert J.D. Work suggests that the likelihood of seeing the "enthusiasm, or talent for participating in an officially encouraged competition" in the West is low.<sup>46</sup> In February of 2022 China cyber expert Dakota Cary indicated that while the Tianfu Cup and competitions like it were likely inspired by the DARPA 2016 Cyber Grand Challenge the U.S. has not hosted another such event since the DARPA event in 2016.<sup>47</sup>

### 3.5 (U) Mandatory Disclosures of Software Vulnerabilities

(U) Chinese cyber researchers are required to disclose their knowledge of software vulnerabilities to the government - which represents an advantage that the U.S. government does not benefit from.<sup>48</sup> Further, due to strict laws and restrictions that govern the release and sharing of information related to cybersecurity in the PRC, one can expect that more research papers on cybersecurity subjects will be available from researchers in the United States. Consequently, examination of open-source search results of cybersecurity-related research papers would be a poor means of comparing the state of cyber R&D between the two countries.

(U) The case of the Mayhem tool for automatically detecting, patching and exploiting software vulnerabilities provides an example of contrast between the U.S. and Chinese willingness to be open about their emerging cybersecurity R&D opportunities. The Mayhem system was demonstrated at DARPA's 2016 Cyber Grand Challenge. The U.S. Department of Defense since adopted the technology - but the Chinese were represented at the same event in 2016 and were



immediately aware of the new technology to be adopted by DoD. The PRC's tighter controls over cyber technology disclosures would tend to prevent this kind of situation from happening where the U.S. would get an early view of a PRC- developed technology to be adopted by the PRC government.<sup>49</sup> The Chinese are anything but shy when it comes to exploiting the technical advances of others. China cyber expert Dakota Cary was quoted as saying "Time and again, China has studied the U.S. system, copied it's best attributes, and in many cases expanded the scope and reach." <sup>50</sup>

### 3.6 (U) Chinese Industry and Cyber Research

(U) A contrast exists between how the U.S. and the PRC work with their IT and cybersecurity industries. Unlike the Americans, the Chinese are not fettered by intellectual property issues affecting their contractors. While the U.S. must observe and protect the intellectual property belonging to their contractors, the Chinese are free to hire multiple contractors and merge the best aspects of each of their approaches into a final product. This effect is only approximated by teaming agreements in the U.S..<sup>51</sup>

(U) Talent residing in the domestic cybersecurity industry in the PRC has the potential to be co-opted by the government through legal or political pressure.<sup>52</sup> With respect to foreign cyber security and IT industries, they can be assured that if their products are relevant to handling or protecting data in any way, the Chinese are actively working to identify vulnerabilities in their products. A United States-China Economic and Security Review Committee (UCESRC) 2022 report cited evidence that there is evidence that Chinese SSF cybersecurity researchers purchase foreign antivirus software ostensibly so it can be used to test the malware they produce. It could also be technically exploited to look for clues that could lead to discovery of new zero-day vulnerabilities. <sup>53</sup>

### 3.7 (U) Military and Academia Coordination on Cyber Research

(U) Adam Kozy, China cybersecurity expert observed that there seems to be a "revolving door" between China's patriotic hacker groups, the PLA, MSS affiliated entities and various private sector companies shown to have worked with Chinese intelligence services.<sup>54</sup> The PRC has developed "world class cybersecurity schools" that emphasize the use of artificial intelligence and other advanced technical approaches. Seven of the schools are referred to as "the Seven Sons of National Defense".<sup>55</sup>

(U) As an example of how weaponized academic institutions in the PRC have become in support of the CCP's cyberspace dominance objectives, and how open about it they are, one can find research papers from Chinese universities that openly advance new research in offensive cyber (and IOs) capabilities. The paper "PPA: Preference Profiling Attack Against Federated Learning" by Zhou, et al advances a method for extracting private information from online shopping and social media users through federated learning profiling based on publicly facing data such as aggregated likes and dislikes and even by scanning the victim's uploaded selfies and classifying their facial expressions. <sup>56</sup> The literature review did not uncover research of offensive cyber technologies being conducted by American universities.<sup>57</sup>

(U) (U) Figure 1 is the FBI Wanted poster associated with the search for hackers from the PLA-associated degree-granting institution named 54<sup>th</sup> Research Institute. The four hackers were indicted by an American grand jury on February 10, 2020. The indictment was related to the hacking and data theft from the Equifax credit reporting agency where the financial records of 145 million Americans.<sup>58</sup>



(U) Figure 1 FBI Wanted Poster for 54th Research Institute Hackers

(U) The Chinese Ministry of Industry and Information Technology (MIIT) and the State Administration of Science Technology and Industry for National Defense (SASTIND) supervise at least 23 universities that conduct cybersecurity research for the PLA. In contrast with U.S. government collaboration with academia on cybersecurity technology R&D, some of the Chinese schools are located on PLA sites and some have already been implicated in state-sponsored hacking operations.<sup>59</sup>

(U) China cyber expert Dakota Cary observes that the Chinese have emulated parts of the United State's cyber-research infrastructure in their own university programs. For example, Cary points out that they developed their cybersecurity degree program based on the NIST "National Initiative for Cybersecurity education". Cary also pointed out that the Chinese program for conferring awards for excellence in cybersecurity education are based on NSA/DHS programs to certify institutions as cyber centers of excellence.<sup>60</sup>

### 3.8 (U) R&D Dependency on Materiel Supply Chains

(U) Cyber technologies are dependent on other technologies including some deemed as critical by DoD (e.g., microelectronics, 5G, AI/ML, batteries, autonomy and quantum). U.S. intellectual leadership in these areas can be considered to be shared or in question. Further, supply chain dependencies and realities where the dominant proportion of specialized and high-performance microchips are sourced by foundries in Taiwan, a contested country only 110 miles off the coast of China.<sup>61</sup> A report from the Institute for Defense Analysis (IDA) indicated that the U.S. will likely need to rely on an unsecure supply chain controlled by other countries in order to meet the need for leading edge microelectronics for advanced weapon systems.<sup>62</sup>

(U) The challenges of supply chain fragility and the results of waning science and technology (S&T) investments appear to aggravate the U.S. more than China. The supply of advanced microchips remains precarious as 75% of global microchip production takes place in East Asia and 90% of the most advanced chips are made in Taiwan. Only about 10% of computer chips are produced in the U.S.<sup>63</sup> While the U.S. relies on Taiwan- which is an existential risk in terms of its continued alliance with the U.S., for advanced microchip fabrication, the PRC is rapidly developing their domestic capability to produce mature and high-end chips. Development of a Chinese microchip manufacturing capability is in the context of an overall "de-Westernization" of the technology supply chains in the PRC. The resulting independence from Taiwanese and other advanced semiconductor markets in east Asia will provide China an advantage over the U.S. in terms of supply chain resiliency and the ability to field new and replacement cyber-enabling hardware.<sup>64</sup>

(U) With respect to rare-earth minerals that are vital to high performance technologies such as <sup>\*</sup>  
<sup>65</sup>:

- Lamp technology
- Laser technology
- *High performance semiconductors*
- High temperature and strength ceramics
- High performance optics

- High performance motors
- High performance batteries
- *Fiber optic technology*
- *Hard Drive technology*

\*Technologies most relevant to Cyber appear in italic font.

(U) The PRC either controls the sources outright or has arranged for strategic cooperation with the countries that source the materials. This is in contrast with the U.S. level of access to these kinds of materials. Evidence suggests that the PRC's defense industrial base for R&D and the supply chain that supports it remain robust. PRC researchers and research teams remain well-represented (if not "over-represented") in S&T literature relevant to critical technology areas.

### 3.9 (U) Diverse Norms of Behavior Impacts to Cyber R&D

(U) When the U.S. seeks to enhance or develop a new cyber capability they must contract and pay for those R&D services as well as any technical resources that are needed and not already on hand. In contrast, the PRC has the advantage of being able to use pirated technology and stolen, proprietary research results, code and system designs. The CCP does not recognize any claims to the products and technologies it is able to acquire from any method of acquisition. In this way, CCP cyber research money can in many cases, be focused solely on areas of new R&D and it need not pay for any pre-existing technology regardless of the technology owner.

(U) The PRC enjoys easier access to early software releases from American telecommunication and software companies while the Chinese government maintains higher degrees of control on Chinese products- making them less available for vulnerability harvesting by their adversaries.<sup>66</sup> The cybersecurity firm Crowdstrike observes that the Chinese affiliated actors are drifting away from traditional exploits such as spear phishing, credential harvesting and compromised websites in favor of attacks on remote services made possible through timely R&D and access to proof of concept enterprise software (ripe for early exploitation).<sup>67</sup>

### 3.10 (U) R&D Capability for Cyberwar Involving Complex Infrastructure Targets

(U) The concept of "Smart Cities" being developed by China effectively embeds sensors and data access points throughout cities. The result is an integrated capability for inward and outward facing surveillance and a test bed for collecting, managing, fusing and exploiting huge amounts of data from disparate sources. The Smart Cities concept has been implemented as part of the Chinese Belt and Road and Digital Silk Road international outreach initiatives.<sup>68</sup> The Smart Cities concept relies heavily on the "Internet of Things" (IoT) concept and as such, the Smart Cities concept has the potential to provide unique and large-scale resources for the study of IoT implementations of OCO and DCO concepts.<sup>69</sup>

(U) The U.S. does not have a comparable effort and as such, the Chinese are realizing a research and development advantage over the U.S. in terms of their abilities to collect, manage, fuse and exploit huge and disparate datasets relevant to large -scale cyber-attacks on and defense of, complex infrastructure targets. In particular, the Smart Cities represent an enormous data collection resource with vast numbers of network access points to support cyber maneuvers and

fires. Further, the data is extremely valuable for training AI/ML enhanced cybersecurity applications.

### 3.11 (U) R&D Focus on Artificial Intelligence and Machine Learning (AI/ML)

(U) As noted in the previous section, the Smart Cities concept can be expected to yield vast amounts of data needed to refine artificial intelligence and machine learning approaches for offensive and defensive cyber operations.

(U) The PRC and Russia both enjoy advantages over the U.S. in their ability to weaponize artificial intelligence for military purposes including cyberspace operations. The USG observes some degree of restriction due to moral and legal norms that prevent it from harvesting the maximum amount of data with which to train AI systems.<sup>70</sup> Dr. H. Kautz of the National Science Foundation observes that "China is pouring enormous resources into ML and has a long history of using cyberattacks for political and economic aims ... Unless the U.S. makes an unprecedented and urgent investment in ML for cyber defense and attack, we will lose the race before it has hardly begun." <sup>71</sup>

### 3.12 (U) R&D Focus Quantum Applications

(U) Cryptography is a key enabler of cybersecurity. Quantum science has strong implications for future cybersecurity related research and development and operational systems. According to the 2020 article by Tom Stefanik of the Brookings Institution entitled "The State of U.S.- China Quantum Data Security Competition", western countries like the U.S. have been focusing on research into quantum computing mostly- and based on commercial advantages perceived by large companies based on computational speed (that has cybersecurity implications involving the ability to break encryption). In contrast, China has focused on cybersecurity applications like Quantum Key Distribution (QKD) based on "deep concern about internet security at the highest level of Chinese leadership." <sup>72</sup>

(U) China has assumed the lead in R&D and deployment of QKD. The Chinese operate the largest QKD-supported network, which boasts a 1200- mile backbone. In 2017, the PRC demonstrated the capability to distribute cryptologic keys from a satellite, to the network.<sup>73</sup> Quantum-distributed keys cannot be exploited by a man-in -the- middle (MITM). They are only good for a single use and then they default to a trivial data mode. QKD - supported networks are vulnerable to denial of service disruption based on MITM attacks where keys would be opened or intercepted and rendered useless on a repetitive basis.<sup>74</sup>

(U) The article by Stefanik suggests that any technical collaboration between the PRC and the U.S. on basic science matters related to quantum data security would be a net benefit for the U.S.<sup>75</sup>



## 4.0 (U) Technology Insertion in China and U.S.

(U) Cyber-related technologies include those that are produced under contract and in association with formalized requirements as well as those that are produced rapidly or even on-the-fly in the context of other cybersecurity- related activities. This section will discuss both of these cases and will point out where distinctions between the two countries lie with respect to technology insertion.

### 4.1 (U) Contrast in Cyber Acquisition Processes

(U) Sections [3.6](#) and [3.9](#) of this document disclose examples of how the PRC codified relationships with industry and adopted norms of behavior provide advantages in research costs. Broad legal authority at the hands of the CCP and relaxed norms of behavior to the point where the Chinese do not appear to even be bound by international law in matters regarding cybersecurity also provide advantages in support of technology insertion.

(U) It's not clear what the Chinese process is for managing requirements as they apply to new cybersecurity tools and products. What can be assumed is that the vast network of contract hackers that work at the behest of the PRC are unencumbered by a formal and lengthy acquisition process. In many cases, it is likely that the contractors are paid based on completion of the operational task at hand and whatever new tools that they might need to meet their objectives are selected from pre-existing tools, modified pre-existing tools or scripted to order by the APT or hacker group.

(U) According to a 2019 Council on Foreign Relations report, the Chinese cyber threat group APT3 was able to take NSA cyberweapons used against them and repurpose them to carry out cyber-attacks against private companies in Asia and Europe.<sup>76</sup> This is a case of the PRC being able to bypass or reduce R&D and test and evaluation processes that would normally apply to the insertion of cyberweapons in order to make the tools operational in a most expeditious manner.

(U) American cybersecurity experts are also capable of producing targeted exploit tools in an expeditious manner- though few details could be uncovered in the literature. The more traditional acquisition process within DoD is not known for being rapid. (U) Table 1 offers a simple model of the timeline for a defense acquisition program. Based on the crude estimates provided in the table, it is reasonable to assume an average time period of about 68 weeks or 1 year and 5 months between the identification of the need and the presentation of a fieldable technology.

*(U) Table 1 Simplified Model of Timeline for Traditional Acquisition Process*

UNCLASSIFIED		UNCLASSIFIED	
Phase of Acquisition		Estimated Time Required	
Recognized need to Issuance of Solicitation to Industry		The MITRE Corporation produced an article entitled "Understanding Government Timelines to Award". This article suggests that the time it takes for the government to recognize it's need until it issues a solicitation is between 3-6 months. For illustration purposes, we will assume an average of 4.5 months. <sup>77</sup>	

UNCLASSIFIED		UNCLASSIFIED	
Phase of Acquisition		Estimated Time Required	
Issuance of Solicitation to Time of Award		A GAO report issued in 2018 reviewed a sample of 129 DoD contracts and determined that while there was great variation in the amount of time between the issuance of a solicitation and award, 68% of contracts were awarded within 1 year of the issuance of the solicitation. For illustration purposes, we will assume an average of 6 months. <sup>78</sup>	
Time of Award to Project Kick-off		The article "The Importance of a Post-Award Kick-Off Meeting in Contract", by Tara Naughton of Contractworks suggests that 2 weeks is a reasonable time interval between award and project kick-off. <sup>79</sup>	
Project Period of Performance		Experience in defense acquisition suggests that 6 months would be reasonable, if not somewhat conservative estimate of a period of performance for a R&D contract associated with a cybersecurity tool or technology.	

(U) The estimate of the U.S. DoD acquisition timeline given above may not reflect additional delays due to cybersecurity compliance regulations such as Defense Federal Acquisition Regulation Supplement (DFARS). DFARS specifies the core requirements for companies that seek to conduct business with the DoD. Cybersecurity is covered under clause 252.204-7012; NIST 800-171 — Based on DFARS, NIST 800-171 provides detailed guidelines for companies to assess their cybersecurity practices and the Cybersecurity Maturity Model Certification, a framework and plan by which DIB organizations can attain the cyber hygiene certification required to be an approved DoD vendor.<sup>80</sup>

(U) The U.S. defense acquisition system allows for funding of technologies with no clear avenues for transition in direct support of the Services. The infamous “Valley of Death” in DoD vernacular is a reference to a virtual boneyard of defense technologies that were funded and at least partially developed- and subsequently unable to attract a user community within the Services. This phenomenon seems unique to siloed and departmentalized decision- making authorities like the U.S. DoD. A centralized decision- making authority like the CCP or Chairman Xi Jinping can be expected to be less likely to research and develop new technologies only to let them fade to obscurity in a kind acquisition limbo or dead-end.

#### 4.2 (U) Civilian-Enabled Technology Insertion

(U) John Costello, the former Chief of Staff at the Office of the National Cyber Director indicates that the Chinese adopt a "People's War" strategy where everyday citizens are encouraged to play a role in a kind of cyber-militia. This provides enhanced opportunities for fielding systems, monitoring and probing networked assets, practicing Techniques, Tactics and Procedures (TTPs) and executing cyber battle damage assessment.<sup>81</sup>

(U) Chapters 1 and 2 of China's National Intelligence Law Article 7 enable the concept of a People's War. They stipulate that "All organizations and citizens shall support, assist and cooperate with national intelligence efforts in accordance with law and shall protect national intelligence work secrets they are aware of." Article 10 states, "As necessary for their work, national intelligence work institutions are to use the necessary means, tactics and channels to carry out intelligence efforts, domestically and abroad."<sup>82</sup>

(U) The SSF of the PLA is a civilian force capability to conduct operations including cybersecurity operations, IOs, communications security and battlefield environment protection. They also serve in the role of integrating and testing emerging technologies including those that are cyber-related.<sup>83</sup>

#### 4.3 (U) Domestic Industry-Enabled Technology Insertion

(U) A case in October of 2018 showed the concept of the People's War at work. It was reported that China Telecom, the 3rd largest telecom and ISP provider in China, had been hijacking network traffic and sending it through malicious servers in order to conduct spying or to intercept credentials. Researchers assess that the China Telecom attacks began shortly after Chairman Xi Jinping of China agreed with President Obama of the U.S., to cease all government-backed cyber operations directed towards intellectual property theft. China interpreted the agreement as only covering military cyber activities so leveraging commercial entities like China Telecom was a logical extension of Chinese malicious cyber activities- made legitimate through the National Intelligence Law and under a People's War doctrine. There is no indication that the same method, referred to as a "Border Gateway Protocol (BGP) Hijack attack" – which effectively weaponizes commercial and private routers and servers- is a method employed by the U.S..<sup>84</sup>

(U) A more recent example of leveraging commercial infrastructure to insert cyber tools took place in March, 2023. Google banned the Chinese e-commerce application Pinduoduo after malware was detected in it.<sup>85</sup>

(U) The Chinese national intelligence laws referenced previously provide the MSS vectors for inserting malware into commercial technology that the U.S. does not enjoy. This represents an advantage in favor of China with respect to ability to insert malicious cyber payloads in victim devices on a large scale.

#### 4.4 (U) Foreign-Enabled Technology Insertion

(U) China has an enhanced ability to leverage foreign information infrastructure to deploy its cyber tools and weapons. The PRC's active engagement in multilateral institutions such as BRICS (Brazil, Russia, India, China and South Africa), the Belt and Road initiative and the Forum on China-Africa Cooperation (FOCAC)<sup>2</sup> remain fertile grounds to promote China's surveillance technologies, expand its influence and to enhance its ability to maneuver and position its cyber assets in key positions in the global cyberspace.<sup>86</sup>

#### 4.5 (U) University-Enabled Technology Insertion

(U) The concept of the People's War and National Intelligence Law Article 7 apply to academia in the PRC. Section 3.7 of this document addresses the close relationship between Chinese academia and Chinese cybersecurity efforts.

---

<sup>2</sup> FOCAC members are all 53 African countries (except Eswatini), China, and the African Union Commission. ([https://en.wikipedia.org/wiki/Forum\\_on\\_China%E2%80%93Africa\\_Cooperation](https://en.wikipedia.org/wiki/Forum_on_China%E2%80%93Africa_Cooperation), Accessed: 8/2/2023)



#### 4.6 (U) Chinese Ability to Insert Technologies Rapidly

(U) The PRC appears to be keenly aware of the time-sensitive nature of newly discovered vulnerabilities and don't want any potential cyber advantage to escape their grasp. Chinese law requires that individuals and companies in China report newly discovered vulnerabilities to the government within 2 days.<sup>87</sup>

(U) The speed with which vulnerabilities are often exploited and the rate at which newly released technologies are compromised suggest that Chinese government-backed hackers develop exploits themselves rapidly and on the fly during operations. Exploits are also acquired from China's extended hacker and cybersecurity research community through such events as the Tianfu Cup hacking competition. Exploits submitted at the Tianfu Cup have later been acquired and employed by China-nexus hackers. The 2022 Global Threat Report by CrowdStrike indicates that there were several instances where Chinese actors "demonstrated an ability to rapidly operationalize public proof-of-concept (POC) exploit code for newly acknowledged vulnerabilities." <sup>88</sup>

(U) During the research there were no cases where references to the time-frame for technology insertion were quantitative and specific. All such references involved subjective terms like "rapid", "quickly" or "immediately". Some references are included in the balance of this section. They suggest to this analyst that the insertion timeframes involved in these cases do not exceed a few days.

(U) The 2023 Global Threat Report by CrowdStrike indicated that China-affiliated threats continued to rapidly adopt and exploit vulnerabilities in enterprise software systems after their release in beta or POC form.<sup>89</sup> The Insikt Group September 2022 Cyber Threat Analysis- China report refers to the Chinese-aligned TA413 threat group as being observed "weaponizing" a vulnerability shortly after discovery and publication. The group also employed new exploit technology.<sup>90</sup> An exploit against Apple iPhones was developed by a researcher for the 2018 Tianfu Cup event. The exploit was used almost immediately thereafter as part of a cyber espionage campaign against the Uyghur minority.<sup>91</sup>

#### 4.7 (U) U.S. Cyber Technology Insertion Time

(U) No references were found that characterized the typical length of time the U.S. would take to insert a new cyber related technology. One reference was found that discussed the length of time required to prepare a specialized cyber infrastructure to support technology insertion and operations. A slide entitled "Today: Manual Infrastructure Preparation Doesn't Scale and Creates Attributable Signatures" in the December 2021 DARPA Signature Management Using Operational Knowledge and Environments (SMOKE) program proposer's brief indicates that the length of time to prepare an (offensive) cyber infrastructure that is attribution-resistant and capable of supporting multiple concurrent operations is measured in "weeks or months." <sup>92</sup>

## 5.0 (U) Offensive Operational Effectiveness

(U) As with any technological discipline, cybersecurity lends itself to description and characterization in terms of metrics associated with its key component functions. LT CDR Tyson Meadors identified five of these metrics in a U.S. Naval Institute article entitled “Five Cyber Metrics Every Naval Officer Needs to Know”<sup>93</sup>. The metrics are:

1. Breakout Time: The time an attacker requires from initial system penetration to obtain lateral access to another host on the system.
2. Dwell Time: The time it requires a cyber defender to recognize an intrusion has occurred.
3. Mean Time to Patch: The average time required to apply a patch once the patch is made available.
4. Mean Time to Contain; The average time elapsed between the detection of an attack and the time at which defenders have eliminated that threats capability of further exploitation.
5. Mean Time to Recover: The average time it takes an organization to return to its pre-attack state- including the additional defensive measures applied during patch and containment processes.

(U) The metrics listed are good for cybersecurity managers to track and assess their own performance. Unfortunately, few of the metric data that would be relevant to this study were available in the literature. If it were, it would be remiss not to include it in the discussions of operational effectiveness and defensive capabilities. In the absence of these data, this chapter will focus on other bases for distinction of relative operational effectiveness in OCOs. Chapter 6 will also address DCO efforts in an abstracted way.

### 5.1 (U) Bases for Distinction of Operational Effectiveness

(U) Nation states and their contractors aren't typically forthcoming with details and data pertaining to operational effectiveness of their OCOs and DCOs. Also, making direct comparisons of the operational effectiveness demonstrated by Chinese and American cyber forces is problematic based on divergent strategic approaches to cyber warfare adopted by each country. Moreover, the scope of PRC offensive operations tends to bias inferences of operational effectiveness towards OCO's while the U.S., faced with a phenomenal number of cyberattacks from the PRC and others, can be expected to be operationally biased toward DCOs.

(U) This chapter deals with the dichotomy by focusing on readily identifiable distinguishing factors that impact operational effectiveness. These factors are grouped into three categories and are presented in order of increasing granularity- from the highest level of conceptual abstraction- to the lowest. The first, “Strategic Approaches” addresses current doctrine and military and socio-economic strategies that can be expected to enhance one side's operational effectiveness over the other. The second category, “Enablers” is at the next lowest level of abstraction. Enablers are practical conditions that can be expected to be drawn upon in order to enhance the operational effectiveness of a country's operational effectiveness. Lastly, the level “Techniques, Tactics and Procedures (TTPs)” is at the lowest level of abstraction and greatest contextual

granularity. It addresses tactical means and approaches that can be expected to impact a nation's operational effectiveness in cybersecurity.

(U) The TTPs referenced in this chapter should not be construed as some kind of summary of Chinese OCOs. A much larger document could be dedicated to the record and evidence of the large-scale cyber incursions into every sector of American industry, government, infrastructure and academia. The OCO's that are referenced here have been included because they tend to represent OCO techniques that appear to be used for the most part, asymmetrically by China against the U.S. (and others).

## 5.2 (U) Defining Offensive Cyber Operations

(U) "State-sponsored offensive cyber operations" have been defined as operations to manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems or networks." <sup>94</sup> OCOs can be purposed towards; industrial espionage operations; military/ diplomatic espionage operations; physical infrastructure attacks; attacks against communication networks; attacks against financial institutions; influence and IOs; and funding through ransom operations. Therefore, operational effectiveness in OCO's can be expected to be correlated with (among other things) the amount of experience executing successful operations in the listed areas.

(U) In the case of OCOs, it is important to consider the distinction of whether the primary objective of a cyber- attack is intelligence gathering (including industrial espionage) or to disable, corrupt, hold ransom, or destroy. A further distinction can be made as to whether the cyber- attack occurs in real time or cyber maneuver takes place such that the offensive function can be triggered on command at a later time- in effect, performing a sleeper-cell role where the attacker lies in wait in cyberspace prior to executing their malicious cyber functions. Attack trends current as of early 2022 not only feature the familiar fast, smash and grab type attacks, but also sleeper type attacks where a large number of infected machines will remain dormant and not draw scrutiny, only to be triggered at a later date to steal, lock or ransom data or to spread their offensive payloads. <sup>95</sup>

## 5.3 (U) Attribution

(U) Any discussion of the relative offensive cyber capabilities of one actor over another should be associated with a caveat that addresses the inherent difficulty in attributing activities in the cyber domain to one entity or another. It is inherently easy to cover one's tracks using proxy servers or to disguise activities to achieve a false flag effect. The "signature" indicators left by one attacker or his/her tools, can be co-opted by another from a different offensive cyber cell. Multiple layers of misdirection can obfuscate the location of origination of attacks. There is an unavoidable level of uncertainty associated with cyberattack attribution that should be considered. At the same time, one cannot remain operationally paralyzed due to some degree of uncertainty. One can accept that the preponderance of the evidence- at least as it applies to the scale, scope and nature of attacks from the PRC- and in the context of the larger picture of strategic objectives- implicates the PRC and CCP-supported offensive cyber cells. For example, the primary antagonist towards Taiwan is the PRC. Those offensive cyber actors engaged in the continuous attacks against Taiwan are most likely Chinese in origin. The same kind of factoring

UNCLASSIFIED

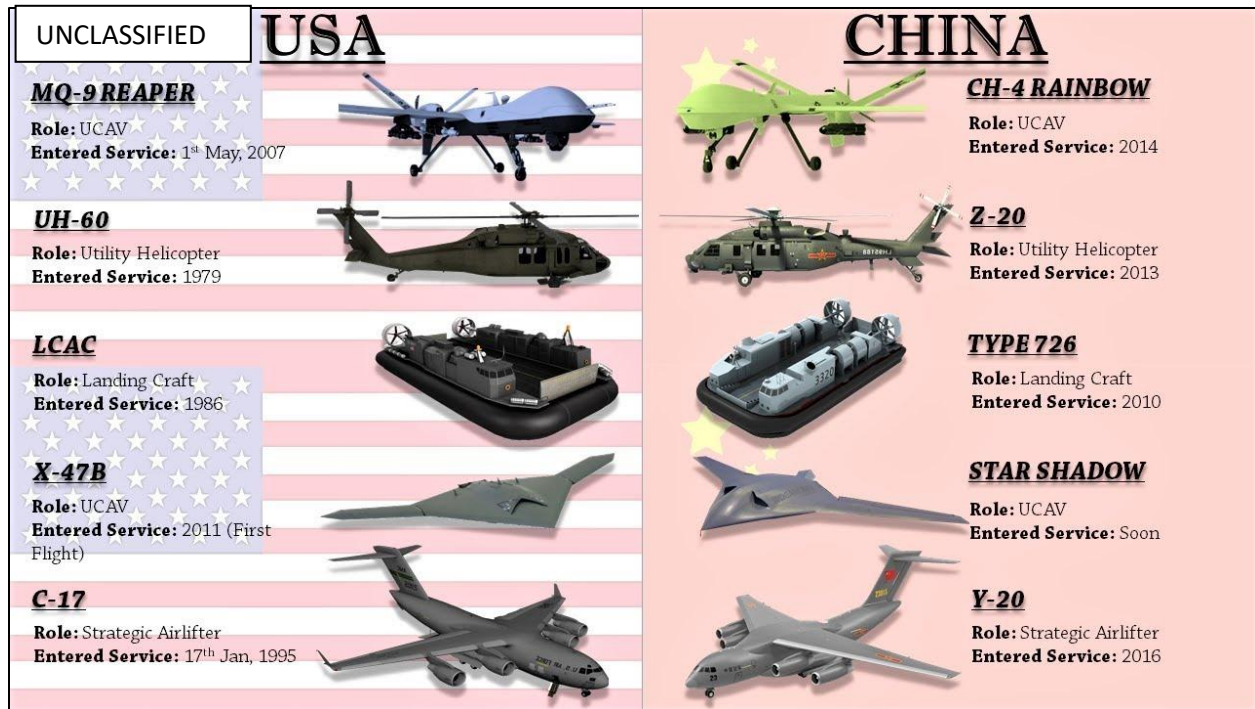
can apply with attacks against the United States. Cybersecurity intelligence experts have become very adept at working within the realms of uncertainty and subterfuge and offer a large amount of useful, if not 100.00% reliable information.

(U) Evidence of OCO's in the form of cyber espionage by China against the U.S. can be found in the form of weapon systems in the hands of the PLA. (U) Figure 2 shows five Chinese weapon systems that appear to be close copies of American weapon systems.<sup>96</sup> While attribution remains a difficult task, one can observe that it is Chinese jet fighters that look like American ones<sup>3</sup> and not vice-versa. It is American intellectual property and capital that tends to be at risk and not Chinese. Also, it is the United States that suffers the most cyber-attacks in general, against infrastructure, financial institutions and information networks. The value of IP lost to China per year has been estimated to be between \$225B-\$600B.<sup>97</sup>

(U) A Newsweek article in September of 2022 provided an example of an attribution of a cyber attack by the United States against the PRC. Chinese cybersecurity experts attributed a cyber attack against the Northwestern Polytechnical University in China's Shaanxi Province to the United States. The cyberattack was based on trojan horse type malware delivered through e-mail. One of the bases by which attribution was made was that no cyberattacks through the malicious software had been observed on weekends or on U.S. holidays. In February of 2022, the Chinese - based Qi An Pangu cybersecurity lab reported that the NSA has been engaged in decade long cyberattacks against 45 different countries including its allies.<sup>98</sup>

---

<sup>3</sup> At the Pacific Operational Science and Technology Conference of March, 2023, Admiral John C. Aquilino said of the new Chinese J-31 jet fighter, "Let there be no doubt that China didn't deliver that capability on their own, It was stolen." The Admiral indicated that the J-31 was the result of the Chinese obtaining American F-35 technical data. (SOURCE: Carberry, Sean. "Dispatches: Speaking of Technology Theft". National Defense. Article. 4/2023, Vol. 833. P 7.)



(Image copied from "10 Chinese Weapons That Were Copied From USA". The Buzz YouTube Channel. Posted: 9/23/2021. Accessed: 5/30/2023.)

(U) Figure 2 Visible Evidence of China Copying U.S. Military Weapon Systems

#### 5.4 (U) Strategic Approach: Network Warfare

(U) The book "Unrestricted Warfare" by Qiao Liang and Wang Xianguan (both PLA Colonels) introduced a strategy by which China, at the time (1999) a weaker country, could defeat a technologically superior foe without needing to rely on hard military power. In the book the colonels identified the US military's main weakness as its dependence on information and communication technology (ICT) networks. Through exploitation of that dependence the PRC could obtain an advantage. So, at least since 1999, China has been preparing to destabilize, demoralize and dominate in confrontation with the U.S. based at least in part, on its ability to employ efficient and overwhelming cyber-attacks.<sup>99</sup>

(U) In 2015 China's Ministry of National Defence issued a paper entitled "China's Military Strategy" where they introduced and emphasized the importance of "informationalized warfare". Cybersecurity figures prominently in this paradigm in that without it, information can be controlled, destroyed, tampered with and held hostage by an adversary. The document introduced the concept of cyberspace to the Chinese population as a "new pillar of economic and social development, and a new domain of national security." China understood then as it does now that cyber capabilities need to be "developed holistically, not only as a response to the evolving cyber warfare approaches and practices of other countries, but also to be in accordance with its national security environment and domestic situation."<sup>100</sup>

(U) The PRC recognizes the concept of "Network Warfare" as a field within cybersecurity that is focused solely on ensuring that networks in the PRC operate reliably and smoothly while the networks of the PRC's adversaries do not. The PRC executes network warfare in the context of gray-zone operations and across the peace-war continuum.<sup>101</sup> The concept of "Network Deterrence" a corollary of network warfare is employed by the PRC to demonstrate their own capabilities within cyberspace and their willingness to apply them. The OCOs are meant to dissuade potential adversaries from engaging in OCOs (or, potentially other offensive operations) against the PRC.<sup>102</sup> There is no indication that the U.S. is also embracing policies like these where the baseline or default state is one of malignancy towards the military and civil information infrastructure of other nations. To the extent that such a malignant approach towards its neighbors in the cyber domain represents an advantage to the aggressor, the PRC would realize the advantage while the U.S. would not.

### 5.5 (U) Strategic Approach: Cyber Force Size

(U) During a U.S. Senate Homeland Security and Governmental Affairs committee hearing on 17 November 2022 FBI Director Christopher Wray stated "On the cyber front, China's vast hacking program is the world's largest by a mile, and they have stolen more of American's personal and business data than every other nation combined."<sup>103</sup> Wray also testified that China's hacking program is larger than the hacking programs of the other major nations -combined.<sup>104</sup> Of 41 APTs referenced in the 2023 Mandiant report "Advanced Persistent Threats (APTs)", 26 were associated with or suspected to be associated with China.<sup>105</sup>

(U) China's most prolific cyberespionage unit, "Unit 61398" (a.k.a., "APT1") is made up of a staff of hundreds or thousands. Unit 61398 requires that its personnel be trained in computer network operations and network security and that they be proficient in the English language.<sup>106</sup> The requirement that the Unit 61398 operators be proficient in English would represent an advantage for the Chinese over Americans- who could be expected to have comparatively few Chinese speakers.

(U) China's PLA and Ministry of State Security (MSS) supplement their ranks of their cybersecurity experts with teams of contractors and hackers hired from industry or recruited from hacker groups. Adam Kozy of the company SinoCyber- that specializes in Chinese cybersecurity intelligence and analysis references the story of Chinese national Tan Dailin (aka "WickedRose" of APT 41) as an example of how the PLA Technical Reconnaissance Bureau scouted Dailin, groomed him, funded him and used him to train and develop others. In this way the MSS maintains a growing number of well-trained and coordinated cyber-mercenaries and hacker cells that serve the MSS as independent contractors by carrying out operations and constantly improving and upgrading tools and techniques.<sup>107</sup>

(U) On the other side of the coin, the Chinese Communist Party organ publication the Global Times reported that the Chinese cybersecurity firm, Qi An Panju Lab had identified four members of a pro-western hacker group named "Against The West (ATW)". The article went on to name one of the hackers- a Swiss national. (Note that none of the ATW hackers were identified as being from the United States). The Global Times reported that the Swiss hacker



was under charges brought by the U.S. Department of Justice (DOJ) for the hacking of more than 100 companies and leaking proprietary information but that the case against the hacker was suspended abruptly after which time, the PRC became the hacker's main target.<sup>108</sup> This case is significant because it appears to be an example of the U.S. employing contractor cyber-criminals to carry out cyber operations against the PRC. The PRC is known to rely a great deal on particularly malicious cyber criminals to carry out official government OCOs. Any country that uses contractor "cyber mercenaries" assumes a risk that those actors could turn on each other in a quest for more or larger contracts or be compromised by a "higher bidder". These kinds of issues are less likely in the more regimented and controlled government- owned cyber force in the U.S.<sup>109</sup>

(U) The ability and willingness of the Chinese government to use non-state actors; contractors and cyber militias in addition to its military and intelligence apparatuses to perform OCO increases their number of attack vectors and enhances their operational effectiveness.

#### 5.6 (U) Strategic Approach: Concurrent Criminal Operations

(U) The PRC's offensive cyber exploits have the potential to pay for themselves in ransom paid by victims with large stakes in data, system availability, logistics and reputation. The Chinese embrace a policy of giving their cybersecurity contractors effective free-reign in terms of expanding on officially sanctioned operations to include extra, potentially lucrative operations whether they involve criminality or not. In fact, the contractor hacking teams hired by the Chinese security services will often raise money by illicit cyber means while also earning money by working for the security or intelligence apparatus. China-cyber expert Dakota Cary indicates that while the U.S. might purchase vulnerabilities from American companies in order to perform OCOs, or use the companies to provide DCO functions, the U.S. Government doesn't hire contractors to perform OCOs.<sup>110</sup>

(U) Officially sanctioned lawlessness during times of conflict is as old as recorded history. The willingness of the Chinese to turn a blind eye to cybercrimes including ransomware attacks, blackmail and theft should be viewed as an advantage that the PRC has over the U.S. in terms of the ability to retain and grow their cyber forces. Furthermore, the illicit tools of blackmail, extortion and theft are not typically associated with cybersecurity operations conducted or sanctioned by western states yet they are frequently utilized by PRC-aligned cyber-forces. This can also be expected to translate to an operational effectiveness advantage for the PRC over the U.S.

#### 5.7 (U) Strategic Approach: Characteristically Active

(U) Executing a Google search on "What country is responsible for the most cyber-attacks?" on 24 March 2023, four sources newer than 2019 were found. Each of them identified the PRC as being the most active cyber aggressor state.<sup>111 112 113 114</sup> PRC -associated cyberthreat actor activities greatly expanded in 2022 according to CrowdStrike Intelligence. PRC -nexus adversaries were observed targeting nearly all global industry sectors and geographic regions CrowdStrike Intelligence tracks.<sup>115</sup>

(U) The PRC has been targeting OCOs against the U.S. for more than 20 years.<sup>116</sup> Yet, as late as 2016, researchers were still postulating about the best way to respond to PRC aggression in general. One such study referenced what the researchers referred to as "cost-effective nonmilitary coercive policy instruments available to the United States to counter Chinese aggression". With respect to OCOs carried out by the U.S. against the PRC, the researchers cautioned that the "risks and costs of retaliation and escalation are considerable."<sup>117</sup> Not until 2018 did the Department of Defense Cyber Strategy state that the U.S. will "defend forward" to disrupt malicious cyber activity at its source, including activity that falls below the level of armed conflict.<sup>118</sup> Consistent with the "Defend Forward" strategy, the U.S. would persistently engage with adversaries such as the PRC in gray and red network space. These engagements would be intended to impose costs on adversaries, cyber terrorists and e-criminals for their persistent attacks on the U.S.. Defend Forward operations should serve as a deterrent to some degree and it should occupy adversary cyber resources on DCO's when they would likely otherwise be engaged in more OCO activities.<sup>119</sup>

(U) To put the relatively new "Defend Forward" strategy in context, the Chinese OCOs against the U.S. began in 1999 during the Kosovo conflict, when the U.S. accidentally bombed the Chinese embassy in Belgrade, killing three Chinese reporters. They attacked again in 2001 after a Chinese fighter plane collided with a U.S. reconnaissance aircraft.<sup>120</sup> While those attacks were isolated in time, concerted, high-stakes and ongoing cyberattacks from China and by "criminal contract hackers " backed by the Chinese government have been attacking the United States regularly since at least since 2011.<sup>121</sup> Five years later the U.S. is still considering ways to respond. Two years after that the U.S. decides that responding with our own OCOs would be fair game. According to the Washington Times, the U.S. hadn't begun OCOs against China until about March of 2019. This was done in retaliation for largescale cyber-enabled intellectual property theft attributable to the PRC. Prior to this point, the U.S. policy was to "name and shame" the Chinese - by legal or diplomatic means as opposed to retaliating in kind. The U.S. OCO was focused on stealing PRC military technology.<sup>122</sup> One might expect that the Chinese are more practiced and more operationally effective based on the more than 19 year gap that it took the U.S. to even arrive at a formal strategy to counter the pervasive cyber threats posed by the PRC.

(U) The U.S. is not alone in its position as a major cyberattack target of the PRC. As far back as 2018 almost 35 percent of cyber-attacks against India were attributed to the PRC. In 2019 over 50,000 cyber-attacks attributed to the PRC were lodged against India.<sup>123</sup> Taiwan, on the other hand, serves as a de facto cyber-assault training ground for the Chinese. PRC-nexus hackers have been harassing, disrupting, paralyzing and stealing from Taiwan's government, financial, transportation, industrial and other networks since 2000.<sup>124</sup>

Despite the PRC 's claims to the contrary- and the ability to point to cyber aggression on behalf of the U.S., all evidence available in the open sources indicate that the PRC is the dominant global cyber bully and that they have the most refined cybersecurity resource pool and cybersecurity defensive posture of any state entity,



(U) Uncertainties associated with attribution and undetected threats aside, if an offensive cyber force is more active, the more likely they are to find and exploit vulnerabilities and the more attack vectors and operational positions they are likely to have in order to carry out exploits. These factors would tend to correlate with an advantage in operational effectiveness for the Chinese over the U.S.

### 5.8 (U) Strategic Approach: Cyber Espionage

(U) The case of the four MSS officers that coordinated with staff and professors at various Chinese universities involved a conspiracy to target victims in a dozen countries including the U.S., Canada, Great Britain and Germany. Infectious disease research facilities handling research related to Ebola, MERS, HIV, Marburg and tularemia were targeted as were the more conventional technology sectors of aviation, defense, shipbuilding and healthcare and biopharmaceuticals.<sup>125</sup>

(U) Several high-profile cyberespionage attacks on the U.S. attributed to the PRC are listed in an NSA/ Cybersecurity and Infrastructure Security Agency (CISA)/ FBI cybersecurity advisory from 10/20/2020. They include: 1.) A PLA hack against the credit reporting service Equifax where trade secrets and the Personally Identifiable Information (PII) of tens of millions American citizens were impacted.<sup>4</sup> 2.) In December of 2018 PRC-nexus cyber threat actors were indicted for executing a large-scale phishing and spear phishing campaign against managed service providers as a means to steal business data and personnel PII. 3) In May of 2020 the FBI and CISA reported that cyber threat actors associated with China targeted and compromised U.S. organization involved with COVID 19 research.<sup>126</sup>

(U) CrowdStrike identifies the likely goals of the CCP's economic espionage mission as a quest for technological independence and dominance.<sup>127</sup>

(U) The U.S. does not self-attribute to OCOs as a matter of policy. However, the Edward Snowden leak of 2014 included documentation that appeared to confirm that the NSA had successfully exploited a vulnerability in a Cisco router and penetrated the Chinese tech giant Huawei's routers where they were able to collect on the data that passed through them.<sup>128</sup>

(U) The Chinese cyberespionage program is large-scale and demonstrated successful. A program of its scale can be expected to benefit the Chinese in terms of operational effectiveness in a number of ways. In addition to the strategic value of the intellectual property stolen, the program could also be expected to:

- Provide an additional avenue by which vulnerabilities can be discovered;
- Provide a network of compromised systems that can support other types of OCOs;
- Provide a training ground for cybersecurity operators;
- Provide a means to expand networks of compromised human assets to support other intelligence operations.

---

<sup>4</sup> (U) This case is discussed in more detail in the context of Information Warfare and Gray Zone activity.

(U) Eric Noonan, the CEO of the cybersecurity firm Cybersheath made reference to the nexus between cyberespionage and other OCOs. In an article discussing a complex cyber-attack executed by the PRC against the infrastructure of the island of Guam, he was quoted as saying; "China is a lot more sophisticated and would presumably be more successful in activating these latent capabilities (i.e., those emplaced during cyberespionage exploits) that are now embedded in many of our critical infrastructures around the globe."<sup>129</sup>

#### 5.9 (U) Strategic Approach: Infrastructure as a Target

(U) The National Counterintelligence Strategy of the United States of America 2020–2022 warns that cyber weapons offer U.S. adversaries a useful means of holding U.S. infrastructure at risk to shape crisis decision-making. OCOs could impact decisions on whether the U.S. were to conduct operations in support of allies or engage in economic engagement that might impede PRC imperatives.<sup>130</sup> According to the 2022 Annual Threat Assessment published by the Office of the Director of National Intelligence, the PRC is "capable of launching cyber-attacks that would disrupt critical infrastructure services within the United States, including against oil and gas pipelines and rail systems."<sup>131</sup> Between 2011 and 2013 alone the FBI was actively tracking PRC attacks against 23 different natural gas pipelines. PRC-nexus hackers gained access to corporate networks connected to industrial control systems. From there they were able to gain access to supervisory control and data acquisition (SCADA) networks for 16 of the 23 gas pipeline systems.

(U) On June 10, 2022, the CISA, NSA and the FBI released a joint advisory detailing a sustained OCO campaign focused on exploiting networking devices used by broad range of large-scale entities in the financial and industrial and public sectors in the U.S. and other PRC adversary nations.<sup>132</sup>

Telecommunications companies - of which many are American- are regularly targeted by PRC affiliated threat groups. The telecommunication companies are considered high value targets due to the direct access they can provide to the telecommunication infrastructure.<sup>133</sup>

(U) Any case where a cyber force has an active hand against a sector where his adversary does not can be expected to be associated with the kinds of advantages that were provided in the bullets in the previous section. No material was found in the open-source literature that suggested that the U.S. targets elements of infrastructure within the PRC. One might endeavor to conclude that the PRC enjoys an operational advantage over the U.S. based on the larger scope of their sanctioned cyber targets.

#### 5.10 (U) Strategic Approach: Leveraging International Cooperation

(U) The PRC's promotion of its surveillance technologies in the context of multilateral institutions such as BRICS, Belt and Road and FOCAC allow the PRC cyber footholds in potentially strategic areas.<sup>134</sup> On the U.S. side, the Defend Forward doctrine also relies on cooperation with partner nations to maximize the ability to collect threat intelligence that can be used to disrupt or eliminate cyber threats facing the U.S.<sup>135</sup>

### 5.11 (U) Strategic Approach: Norms of Behavior

(U) Adam Segal, the director of the digital and cyberspace program at the Council on Foreign Relations testified before the UCESRC that the United State and China lack a common understanding of what appropriate thresholds are for implementing and escalating OCOs and what constitutes a proportionate response.<sup>136</sup> Such a condition serves as a meaningful deterrent against cyber aggression directed toward China. In contrast, the U.S. tends to embrace the concept of measured and proportionate responses to aggression.

(U) Another advantage in operational effectiveness can be expected based on the effective deputization and de facto control over of the entire country of China in support of China's cyber dominance (or CCP objectives, for that matter). This can be considered a departure from the norms that any human rights- aware country would embrace.

(U) The UCESRC reported in its 2022 report to Congress that "China enjoys an asymmetric advantage over the United States in cyberspace due to the CCP's unwillingness to play by the same rules...". They go on to point out that the two countries diverge sharply on the norms that would guide responsible state behavior in cyberspace during peacetime. The main points of contention are China's perpetration of cyberespionage for economic advantage, its emphasis on state control over the internet under the guise of cyber sovereignty, and its rejection of the application of international law in the cyber domain.<sup>137</sup>

(U) The U.S. has long held the position publicly that international law should apply in cyberspace. This position involves realization that certain constraints exist on the U.S. in terms of offensive cyber activities that would not apply to China- as China does not hold that international law should apply to cyberspace. Failure of the U.S. to adhere to the self-imposed higher standard for behavior in cyberspace would damage the credibility of the U.S. and leave an open door for other entities in cyberspace to ignore behavioral norms in cyberspace that might be widely held even if not universal.<sup>138</sup>

(U) The American position on cyber norms of behavior is tricky. Afterall, who has the better credibility: The actor who makes no claim that they will observe a set of constraints against malicious cyber behaviors and uses the behaviors or an actor that makes the claim that they will observe a specific prohibition on a malicious behavior and can be shown to have gone ahead and used it anyway?<sup>139</sup> Whatever amount of credibility that the U.S. still holds in this area since the Snowden disclosures, they appear hold tenuously.

### 5.12 (U) Enabler: Cyber- Enabling Laws

(U) China's ability to discover vulnerabilities and exploit them, while simultaneously defending their own critical IT infrastructure can be expected to continue based on laws enacted in 2017 that give the Chinese government more authority to co-opt commercial data and resources. Also, China's emphasis on recruiting of cyber talent and formalizing avenues of cybersecurity education can be expected to ensure a steady stream of human resources available backfill and grow the Chinese cyber force.<sup>140</sup> The UCESRC went as far as to state that China's cybersecurity

legislation effectively "weaponizes the country's cybersecurity industry and research" by virtue of the strict requirements that all software or hardware vulnerabilities be first communicated to the government before they are provided to others who could potentially patch them or take mitigating actions.<sup>141</sup>

(U) While China has adopted laws that are very favorable towards their quest for cyber- or network dominance, there is little risk if any to any party acting on CCP directions – whether or not those directions might be legally sanctioned. John Costello, the former Chief of Staff of the Office of the National Cyber Director indicates that through the extralegal status enjoyed by the CCP, the influence over state cyberoperations cannot be overstated. The PLA and MSS have almost unchecked power to co-opt or compel assistance from any Chinese citizen or company.<sup>142</sup> They also have the will and financial resources to gain leverage and influence globally in such a way that affords them advantages that are not likely to be enjoyed by the U.S. or the West.

(U) In the United States, the 2019 National Defense Authorization Act (NDAA) specifically authorizes offensive cyber operations by virtue of the following language: "It shall be the policy of the United States, with respect to matters pertaining to cyberspace, cybersecurity and cyber warfare, that the United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter, if possible, and respond to when necessary, all cyberattacks or other malicious activities."<sup>143</sup>

(U) There were no references to legal standards by which the U.S. government could compel private citizens or companies to cooperate, assist or support national cybersecurity objectives. In this respect, cyber-enabling laws would represent an advantage for China over the U.S.

### 5.13 (U) Enabler: Domestic Surveillance

(U) Surveillance can be a means of enforcement of censorship and compliance with CCP dictates in China. Through censorship, the Chinese population are restricted in what they can see and learn, as well as what they can express. The surveillance state has the effect of conditioning a population to accept the versions of reality that meet the objectives of the CCP. China leads the world in applying surveillance and censorship to monitor its population, to repress dissent and to promulgate communist party messaging.<sup>144</sup>

(U) Americans might recall that the infamous leaking of NSA contractor Edward Snowden in 2013 (appeared to) reveal that the NSA was engaged in sweeping surveillance operations and data collection programs against foreign entities as well as American citizens. Later, Snowden disclosed that the NSA had been executing a cyberespionage campaign against the Chinese company Huawei- ostensibly to determine the extent of its ties with the Chinese military. Similarly, in 2017, WikiLeaks leaked documents purported to show the extent of U.S. Central Intelligence Agency (CIA) involvement with digital surveillance against international targets. The digital surveillance included hacks against traditional telecommunication and digital networks but also cellphones, television sets and automobiles.<sup>145</sup>

UNCLASSIFIED

(U) A domestic surveillance program can have positive ramifications for the operational effectiveness of OCOs. These include:

The ability to access spaces in cyberspace that would otherwise be considered private- such that the spaces can host cybersecurity tools.

The ability to intercept communications so risks to cyber operations might be found and mitigated.

The ability to steal/acquire cybersecurity-relevant resources.

The ability to support censorship operations that serve to shape public opinion in ways that support cybersecurity objectives.

The ability to dissuade or repress individuals from acting against CCP interests in cyberspace.

(U) Domestic surveillance as practiced by both countries are different in that the Chinese surveillance operations are used in support of a strict domestic censorship program and in an officially acknowledged “social credit scoring system”. The degree of censorship practiced by the government in the United States does not approach the level that is practiced in China. For this reason, the existence of a strict domestic surveillance program can be considered an advantage for the PRC.

#### 5.14 (U) Enabler: Drawing on Civilian Institutions

(U) The PRC's cyber-operational readiness is in part, enabled by the concept of military-civil fusion. The Chinese SSF, a kind of “cyber militia” can mobilize Chinese civilian Information Technology (IT) infrastructure elements such as data centers and telecommunications links and nodes and can draw on human talent normally engaged in the Chinese civilian IT sector.<sup>146</sup> The SSF are permanent groups that operate at the discretion of the PLA. The cyber militias will likely support network attack, network security, public opinion monitoring and IO.<sup>147</sup>

(U) The United States does not have a civilian cyber-militia force that supports its armed forces or intelligence services.

(U) With respect to private industry, the Chinese government's "military- civil fusion approach has some positive ramifications for Chinese start-ups and small businesses. The Chinese government has recognized start-up companies and smaller firms as "critical sources of innovation" and have worked to engage with the companies and foster their growth.<sup>148</sup> In July of 2021 the CCP drafted a 3-year action plan in order to strengthen its cybersecurity sector.<sup>149</sup>

(U) Another example of military-civil fusion in the use of civilian cybersecurity- specializing contractors to support cyber operations by the PLA or MSS.

(U) With respect to academia, the arrests of an MSS intelligence officer and a top-ranking official at Nanjing University on cyberespionage charges in 2018<sup>150</sup> is an example of how

Chinese universities assist the MSS and PLA in OCOs in a manner that has no analogue in the U.S..

#### 5.15 (U) Enabler: Drawing on Civilian IT Infrastructure

(U) While the CCP and the military and intelligence organizations that it controls enjoy dominating authority over private industry resources and its own information technology (IT) infrastructure, Chinese observers often decry “U.S. internet hegemony”. “Internet hegemony” is a reference to the perceived dominance over the internet that the U.S. purportedly enjoys by virtue of the fact that many of the routers and servers and software used to support internet functionality are manufactured or controlled by U.S. companies.<sup>151</sup> The four largest cloud services providers: Amazon Web Services, Google Cloud, IBM Cloud and Microsoft Azure are all American companies. This can be expected to benefit the U.S. in terms of the potential for enhanced access for U.S. cyber forces.

(U) The concept of "internet hegemony" notwithstanding, there is no indication in the open-source literature that the U.S. enjoys a comparable level of influence over its information technology sector that China does or that there are any broadly accessible secret backdoors or functionalities built into U.S. produced networking technologies that could be leveraged by the U.S. in a time of war.

(U) On the other hand, China cyber expert Dakota Cary suggests that China might be exploiting agreements or compromises of telecommunication giants in order to collect directly from the internet backbone or undersea cables. These covert access points would afford them operational advantages.<sup>152</sup>

(U) Another consideration relating to operational effectiveness and civilian IT infrastructure has to do with the availability and openness of the technical standards that underpin western IT infrastructure and digital communication protocols. The extent to which a cyber adversaries networking technology is known and understood, makes that system more vulnerable to exploit. Western IT standards are well known and widely available. In contrast, the PRC is engaged in a concerted effort to move away from western technical standards in favor of standards that they develop organically.<sup>153</sup>

#### 5.16 (U) TTP: Cyber in Context with Gray-Zone Tactics

(U) "Gray zone tactics" are coercive actions that fall short of armed conflict but beyond normal diplomatic, economic, and other activities. Gray zone tactics constitute "Military Operations Other Than War (MOOTW)".<sup>154</sup> China has a number of gray zone tactics other than OCOs. The Chinese tend to apply gray zone tactics in layers and across multiple domains (including the economic, information and cyber domains). The end result is a destabilizing influence that favors China without China having to escalate too dramatically (i.e., into warfare) in any single domain.<sup>155</sup>

(U) A 2021 study by Paul Stockton of Johns Hopkins Applied Physics Laboratory states that in a confrontation with China over the highest of stakes, the PRC's doctrine would be one to include OCOs combined with IOs at the outset of an armed conflict. The IOs would be tailored to erode

US confidence and morale among political leadership and the population. The study notes further that cyberattacks alone are poorly suited for communicating coercive threats and related messaging.<sup>156</sup> Chinese military literature discusses the use of cyber to support IOs designed to degrade or shape an adversary's decision-making processes through injecting false information, accessing information systems, and controlling or destroying data. Cyber-enabled IOs would also be used to undermine credibility in the national and international arenas and to negatively impact the morale of the population and to achieve deleterious economic effects.<sup>157</sup>

(U) The 2021 RAND report entitled "Chinese Disinformation Efforts on Social Media" indicates that the CCP is engaged in (cyber-enabled) "narrative-shaping; public opinion management; influence operations; and information warfare, including disinformation campaigns".<sup>158</sup> Thus, while the Chinese uses of e-mail and social media might be technically legitimate and not constitute an OCO against a network technology- the uses might still be part of gray zone tactics associated with malicious intent. Chinese disinformation can be expected to discount the scale of cyber risk posed by the Chinese and others. IOs can serve as enablers of OCOs if they serve to attract potential cyber victims to malicious websites or make them more likely to download or click on malware. The willingness and capability to conduct broadscale IOs that have the effect of reinforcing the effectiveness of OCOs represent an advantage in favor of China.

(U) Chih-yun Huang, a cyber threat intelligence analyst with the Taiwanese cybersecurity firm Team T5 indicated that Chinese cybersecurity firms are releasing detailed threat intelligence reports on alleged U.S. cyber exploits, but they are not being found written in English. Ms. Huang suggests that the reports might be blatant propaganda efforts intended to create anti-American sentiment within the Chinese population.<sup>159</sup>

(U) China's cyber espionage capabilities are enhanced by the integration of offensive cyber capabilities with conventional intelligence gathering and related tradecraft. The MSS actors engaged in cyberespionage operations are not limited to people peering into computer monitors. They include the human agents trained to exploit, influence and recruit useful targets.<sup>160</sup> Dean Cheng, a former fellow in Asian Studies at the Heritage Foundation made reference to reports that the PRC's SSF has integrated the PLA's "311 Base" psychological warfare organization under the Network Systems Department. This would signal an intention on the part of the PLA to maximize the impact of cyber operations on human victims by eroding trust and confidence in leadership and a will to resist. The integrated psychological and cyber-attack approach can be expected to yield an enhanced effectiveness for Chinese OCOs where the psychological warfare objectives of fear and demoralization are met concurrently with the destructive technical and associated economic effects of a cyber-attack (or cyber warfare campaign).<sup>161</sup>

(U) There was no reference in the literature that the U.S. is heading towards an integration of cyber resources with those of IO or psychological operations (PSYOPS) resources or that such an integration would even be effective against the Chinese based on their tight controls over the information that their citizens are exposed to. To the extent that both the U.S. and China might gain advantages through controlling their cyber-related media messaging and shaping the impressions of those that receive the messages, China would appear to have an advantage over the U.S. by virtue of their more complete control over their news and media sources.



(U) The massive data hacks of the U.S. Office of Personnel Management (OPM), Equifax and the discrete dating site, Ashley Madison can be considered an example of information warfare at play. With those data, China can identify what government employees might be ripe for recruitment based on debt or blackmail based on extramarital affairs.<sup>162</sup> This suggests that another distinction can be drawn between U.S. and Chinese operational approaches to cyberattacks. While presumably, the U.S. is working to defend critical information infrastructure with technical means and to conduct OCOs against adversaries, the Chinese are working to exploit human vulnerabilities such that at some point they will have an increased likelihood of flipping a disillusioned, financially strapped or otherwise susceptible to compromise DoD or U.S. intelligence community insider so they might hand over the network keys directly.

(U) American children are not safe from gray zone attacks in the form of IOs intent on demoralization. The popular Chinese video posting app “Tik Tok”, aside from being a data harvesting tool has been found to have an even more sinister purpose. The TikTok algorithms promote sexualization, gender fluidity, discontent and “the blackout game” to American children while Chinese children of the same ages are receiving content directed towards STEM subjects, architecture, music, and the like.<sup>163</sup> The U.S. is not innocent of supplying poor taste, low-brow or destructive content outside its borders. To argue the contrary one would need to defend decades of American television, movies and popular music. American “Big Tech” companies like Facebook, YouTube and Google clearly use algorithms to tailor searches and the feeds of their subscribers. But there is something particularly pernicious about the Chinese targeting their adversary’s children to receive psychological payloads that they know are harmful.

#### 5.17 (U) TTP: OCOs as Elements of Complex Attacks

(U) Some Chinese analysts and media sources make reference to China’s ability to successfully layer diplomatic, administrative, economic, media and nongovernmental activities such as cyberattacks, supported by military deterrence as a model that they have used successfully and will likely use in the future.<sup>164</sup>

(U) When considering the operational effectiveness of Chinese OCOs one should consider that the PRC can be expected to apply OCOs in the context of a wider, multi-dimensional attack that can include coordinated IOs, overflight incursions, diplomatic pressuring, economic pressure, sabotage and other gray zone tactics. These tactics, while they may fall short of the commonly held definitions of warfare held by the U.S., can be expected to distract or confuse the U.S. leadership and population, damage national credibility and morale, strain international alliances and impress economic pressure on the population and the government. The specific impact of OCOs would be difficult to assess apart from the other offensive measures.

(U) The U.S. might be inclined to engage in their own highly integrated, multi-dimensional strategic efforts against the PRC, but the economic, industrial, political and societal conditions vary greatly between the two countries. One might conclude that American society is more vulnerable to these kinds of complex attacks than the highly controlled Chinese society is.

(U) It is easier to imagine the U.S. engaged in a reactive mode focused on retaliating in the political, economic and cyber domains. Such divergent complex attack concepts between the two



countries aggravates the ability to assess the operational effectiveness of the OCO elements of the complex attacks. Comparisons of operational effectiveness based on a domain-by-domain assessment would miss the strategic and tactical benefits of executing a complex attack entirely. In such cases, the whole is greater than the sum of its parts.

(U) The objectives of the application of the cyber methods would be significantly different from the Chinese and American perspectives. The Chinese might measure their operational effectiveness based on how effective their OCOs were in the context of a larger, multidimensional integrated campaign while the U.S. would measure their effectiveness in terms of how one act of retaliation or a limited coordinated effort was able to achieve a set of more limited objectives. Comparisons under such conditions would tend to lack validity.

(U) In summary, in an “apples to apples” comparison of the operational effectiveness of OCOs in the context of complex attacks the Chinese should be considered in the advantaged position based on the increased vulnerability to westernized societies to the (example) complex attack elements mentioned earlier. To focus solely on the operational effectiveness of the OCO elements to draw a comparison is likely to lack validity based on contrasting objectives between the two adversaries.

#### 5.18 (U) TTP: Vulnerability Mining

(U) The PRC has in effect "Cyber Weaponized" its commercial sector in order to among other things, enable a domestic pipeline of software vulnerabilities. This industrial approach to vulnerability discovery gives China advantages in operational effectiveness in cyber operations.<sup>165</sup> An enhanced ability to discover software vulnerabilities not only affords the PRC advantages in OCOs, they are also first to be able to uncover vulnerabilities that will allow them to be more effective in DCOs as well.

(U) CrowdStrike reported that Zero-day exploits (i.e., those exploits that are new and no patches have been issued for them) were most commonly observed in attacks against North American interests and that China-nexus adversaries were able to compromise entities in the aerospace, legal and academic sectors using them.<sup>166</sup> Kelli Vanderlee, an intelligence analyst at Mandiant testified to the U.S. Congress in 2022 that Chinese government-backed hackers have exploited more zero-day vulnerabilities than any other nation.<sup>167</sup>

(U) In 2013 Bloomberg reported that Microsoft was providing the NSA with information about newly discovered vulnerabilities in its software so the NSA would have time to exploit them before patches were issued.<sup>168</sup> A 2016 article in the cybersecurity blog "TechDirt" referenced a case where the NSA was hacked and zero-day exploit tools were taken by hackers and later sold. It was reported that some of the exploits that were stolen and later appeared for sale were exploiting vulnerabilities that were 3 years old. This suggests that the NSA, having learned of a vulnerability, may opt to sit on that information- keeping it from the software vendors even- for as long as it might be of use to them.<sup>169</sup>

(U) There is no indication in the open-source literature that the United States leverages these kinds of advantage at the industrial scale that China does.

### 5.19 (U) TTP: Leveraging Civilian Computers

(U) Botnets are networks of infected computers or routers that can be commanded to execute malicious functions as an orchestrated group. The French cybersecurity research agency Computer Emergency Response Team-France (CERT-FR) indicated that the China-backed APT31 leverages botnets in order to use them as anonymization relays to hide their reconnaissance and other malicious cyber activities.<sup>170</sup> Chinese APTs have been known to employ botnets to execute cyber reconnaissance, attack source obscuration and to execute broadscale cyberattacks.<sup>171</sup>

(U) Botnets are a means by which PRC cyber threats have been known to carry out coordinated attacks using a large number of computers. These “federated” attacks are typically executed at a low intensity and with maximum stealth at first, until a maximum number of computers can be federated into the botnet. As the botnet grows, the intensity increases until it becomes clear that the vulnerability has been discovered. At that time the full federation is brought to bear in order to exploit the vulnerability hastily and to the fullest extent possible.<sup>172</sup>

(U) Federated attacks made possible through botnets can be devastating. The MIT Technology Review article by Patrick Howell O'Neill recounted what he referred to as a "massive hacking spree" carried out by China against Microsoft Exchange servers. He went on to describe the event as demonstrating "Beijing's ability to coordinate an offensive so large in scale that it seemed chaotic and reckless to outside observers." The attack effectively "left a door wide open" on tens of thousands of e-mail servers.<sup>173</sup>

(U) In June of 2022, Robert Joyce, the Director of Cybersecurity at the NSA remarked at the RSA Conference that China is attacking routers and virtual private networks in the U.S. in order to stage themselves within service providers of targeted victims. The Director went on to say that all levels of technology from small or home office technology through large enterprise technology are being attacked. At the same conference Director Joyce indicated that it is the NSA's policy to seek out cooperation with the U.S. data networking industry to help provide tips to help identify threats and trace them to their origination.<sup>174</sup> Both the U.S. and the Chinese accuse each other of establishing and leveraging broad infrastructure networks from which to stage cyberattacks.<sup>175</sup> <sup>176</sup> The literature does not show evidence of the U.S. routinely (or ever) using the networked assets of civilians in their cyberattack chains and so this tactic - an effective tool in the arsenal of the Chinese, represents an advantage to the PRC.

### 5.20 (U) TTP: Supply Chain Attacks

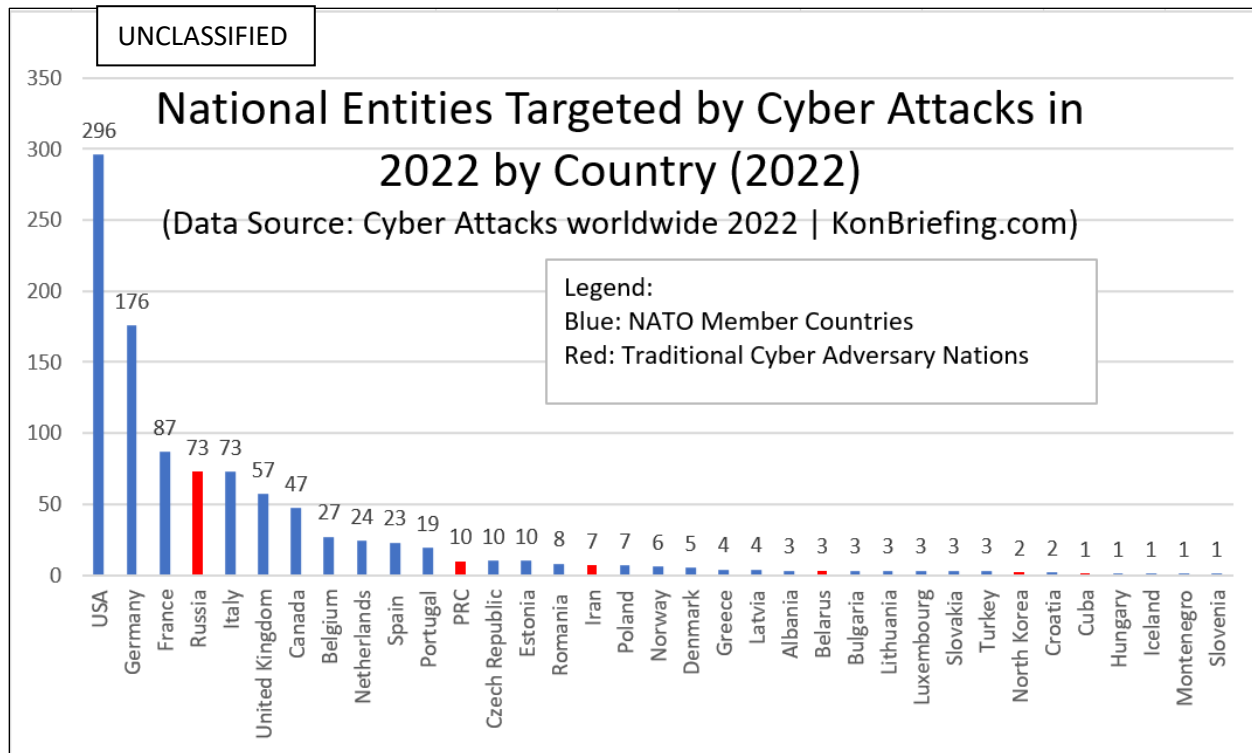
(U) Chinese researchers have developed a sub-industry of sorts in order to penetrate and manipulate open-source code libraries so hidden vulnerabilities will be built-in to a wide range of emerging applications- effecting supply chain attacks.<sup>177</sup> An April 2023 article on SecurityWeek.com reported that the Chinese-backed APT "Evasive Panda" delivered the MgBot multifunctional malware through legitimate update channels- either through a supply chain attack on the update servers, or through man-in-the-middle attacks through compromised internet infrastructure.<sup>178</sup> There were no examples in the literature of the U.S. using the same type of

attacks on commercial product lines to create a vector to support OCOs so supply chain attacks can be considered an advantage for China, in terms of operational effectiveness.

### 5.21 (U) Comparative Assessments in OCOs

(U) (U) *Figure 3* shows the relative number of commercial, academic and government entities reporting cyberattacks during 2022 by country. The chart also shows NATO aligned and NATO adversary status by virtue of blue and red colors, respectively. If the number of entities within a country that report cyberattacks is considered a metric, the data tells us that the ratio of NATO country entities reporting cyberattacks is almost ten times that of the NATO-adversary nations (943 vs. 96). 296, or 31% of the 943 entities aligned with NATO that reported attacks were American. In contrast, only 10 Chinese entities reported being victimized directly, again, a ratio of about ten to one with the US on the defense against unattributed aggressors in this case. Another take-away from (U) *Figure 3* might be that US cyber activities can be assumed to be more defensively oriented while those of China would likely be more offensively oriented.

(U) The reported history of CIA and NSA cyber exploits against China shows that the offensive cyber operations between China and the U.S. go in both directions. The Chinese cybersecurity company Qihoo 360 and the Chinese National Computer Virus Emergency Response Center indicated in 2022 that the NSA's Tailored Access Operations group is responsible for at least 10,000 cyberattacks against Chinese targets <sup>179</sup>. Nevertheless, the open-source reporting indicates that the scale of cyber aggression between the two countries is not at all balanced. Reading from English language open-source documentation from within the U.S. would suggest that the Chinese are disproportionately responsible for OCO's globally. Even as far back as 2014, former NSA Director ADM Michael Rogers testified that China had compromised the U.S. power grid through intrusions that left behind back doors that could be used to wreak havoc in a crisis. <sup>180</sup>



(U) Figure 3 Number of Entities Reporting Cyber Attacks in 2022 by Country<sup>181</sup>

(U) The number of entities reporting cyberattacks is only one potential measure of a cyber forces operational effectiveness in delivering OCOs. The Harvard Belfer Center and the International Institute for Strategic Studies (IISS) identify the following as bases for comparing cyberspace dominance: (advanced cyber-related) military strategy and doctrine; offensive cyber capability; cyberespionage capability; independence on foreign IT and high-tech exports; the scale and quality of the domestic cybersecurity industry; the supply of skilled employees in the IT sector; the percentage of the population that uses the internet; and leadership roles in global cyber governance venues.<sup>182</sup> This analyst would add: Demonstrated ability to execute OCOs on multiple concurrent fronts; Demonstrated ability to coordinate OCOs with IOs, diplomatic efforts or other domain operations; Demonstrated experience and success rate of OCOs and DCOs; Dedicated and distributed cybersecurity infrastructure; Dedicated, large-scale cyber training operations and, Cybersecurity defensive posture of the nation's key networks and information systems.

(U) While these bases for comparison might be valid, some of them are not objectively reported on in the literature and need to be considered qualitatively. The objectives of this study and document include finding information relevant to these bases for assessment and presenting qualitatively derived conclusions based on them. Also, it should be considered that it is the nature of cybersecurity and defense matters in general, that the full corpus of information about capabilities and willingness to apply them is rarely available.

(U) Some analysts use the different levels of investment in cybersecurity at the national level as an indicator or cyber capability. This analyst urges caution with respect to employing that

approach. Comparing government investment levels in support of cyberspace dominance objectives is inherently risky due to potentially contrasting economic conditions, monetary policies and shifting national priorities and governance prerogatives. Winnona DeSombre, a research fellow at the Harvard Belfer Center, indicated that some analysts will exhibit a “fallacy of sophistication,” where a cyber force is deemed inferior based on a perceived lack of sophistication of the choice of tools.<sup>183</sup>

(U) The UCESRC suggests that the number of vulnerabilities that a cyber force has exploited is an objective and quantitative measure of comparison between the U.S. and Chinese offensive cyber capabilities. The UCESRC observed that reporting from multiple cybersecurity reporting firms indicates that China is the global leader in vulnerability exploitation and that it has exploited more zero-day vulnerabilities than any other nation during the periods of 2012 to 2021.<sup>184</sup>

(U) There is detailed technical reporting that can be drawn upon for additional quantitative analyses. Mandiant attributed 937 command and control servers hosted on 849 distinct IP addresses in 13 countries, over a two year period, to APT1, a single China-based APT.<sup>185</sup> APT1 was able to compromise 17 victim networks spanning 10 different industries in a single month. On average, APT1 enjoys a dwell time<sup>5</sup> of 356 days.<sup>186</sup> While these technical metrics are anecdotal and one-sided, they remain an example of the kind of data that could be used as a basis for quantitative comparisons of operational effectiveness in OCOs.

(U) Another means of assessing the relative operational effectiveness between two cyber forces is to listen to the clearly stated assessments of experts in the field. During the course of this study several statements were found that address the US and Chinese cyber capabilities. They are provided in the following bullets. (NOTE: The author urges caution when interpreting broad statements about which country is ahead of another country in terms of cybersecurity. There are multiple factors to consider and not all analysts will judge each factor or weight them the same.)

- The case of the Office of Personnel Management breach of 2015 offers a rare glimpse of the comparison of OCOs between the U.S. and China from the perspectives of our highest placed intelligence officer at the time. According to an account by Ellen Nakashima of the Washington Post, in response to the successful Chinese exfiltration of 21 million personnel records and 5.6 million fingerprint records (then) National Intelligence Director James Clapper “expressed grudging admiration for the OPM hack, saying U.S. spy agencies would do the same against other governments.” To this date there has been no evidence that such an attack against the Chinese has been attempted or has succeeded.<sup>187</sup>
- Cybersecurity company Margin Research assesses that Chinese domestic cybersecurity companies “increasingly stand at the forefront of their fields, offering insight and services that are not only unparalleled in their scope, but that also represent a tremendous potential resource for China’s government and military.”<sup>188</sup>

---

<sup>5</sup> (U) “Dwell time” is the time an attacker is able to remain on a compromised system until the exploit is discovered and protective measures are taken.

UNCLASSIFIED

- Winnona DeSombre, a research fellow at the Harvard Belfer Center offered congressional testimony that China's OCO capabilities " rival or exceed" those of the United States.<sup>189</sup>

(U) The following statements addressed the rate at which the PRC is advancing their cyber capabilities:

- Margin Research assesses that China's cyber capabilities are improving at an "unparalleled pace". Further, they indicate that "Experts in China stand at the forefront of vulnerability research and have strong insight into the offensive and defensive techniques necessary to combat potential infiltration and exploitation." <sup>190</sup>
- In their 2022 report, "China's Cyber Operations: The Rising Threat to American Security", Margin Research declared that "China's cyber capabilities and operations have increased exponentially to the point where they pose a highly significant national security threat to the United States and all China's perceived adversaries." <sup>191</sup>
- Ms. Lina Lau, Principal Incident Response Consultant for Secureworks indicated in early 2022 that the current state of Chinese cyber capabilities (as advanced and well-integrated as it is), is only elementary compared to what it will become.<sup>192</sup>
- In March of 2023, Lt General Scott Berrier, the Director of the Defense intelligence Agency observed that the Chinese were "advancing very, very rapidly in every war fighting domain"- including cyber.<sup>193</sup>

(U) The UCESRC attributes China's "astounding improvement" in cyber capabilities since 2013 to<sup>194</sup>:

- 1.) the sustained attention to cybersecurity by the highest levels of the Chinese government;
- 2.) the major reorganization of cyber-relevant institutions;
- 3.) substantial investments into its cyber security workforce.

(U) There were quotes found where experts placed the U.S. ahead of the PRC in cyber capabilities. In particular;

- The IISS assesses that the U.S. exceeds China on most metrics of cyber power and in particular in its ability to employ sophisticated surgical offensive capabilities at scale.<sup>195</sup>
- Perhaps in a self-serving statement, a spokesperson for the Chinese government said in September of 2022 that "As the country that possesses the most powerful cyber technologies and capabilities, the U.S. should immediately stop using its prowess as an advantage to conduct theft and attacks against other countries, (and) responsibly participate in global cyberspace governance and play a constructive role in defending cyber security." <sup>196</sup>

(U) Considering the factors mentioned previously and taken in the aggregate and in the context of the information that is currently available in the public sources, this analyst assesses the

People's Republic of China as having an operational effectiveness of their cybersecurity capabilities in excess of those of the United States.

## 5.22 (U) Conclusions

(U) This chapter identified factors in terms of strategic approaches, enablers and TTPs that can be considered to be relevant to a cyber forces operational effectiveness. (U) *Table 2* lists the factors addressed in this chapter together along with columns indicating whether an advantage is held by either the U.S. or China in terms of each factor. A dashed line indicates that no advantage is realized and a check indicates whether an advantage exists and which country enjoys the benefit. The assessments in the table are from the analyst and are based mainly on a review of open-source materials. Supporting discussions are in the relevant sections of this chapter.

(U) *Table 2 Factors Impacting the Operational Effectiveness of a State Cyber Force*

UNCLASSIFIED		UNCLASSIFIED	
Section	Factor Contributing to Operational Effectiveness in Cyber Operations	Advantage of State Cyber Force based on Contributing Factor	
	Strategic Approach	United States	China
<a href="#">5.4</a>	Network Warfare	---	---
<a href="#">5.5</a>	Cyber Force Size		✓
<a href="#">5.6</a>	Concurrent Criminal Operations		✓
<a href="#">5.7</a>	Characteristically Active in OCOs		✓
<a href="#">5.8</a>	Cyber Espionage		✓
<a href="#">5.9</a>	Infrastructure as a Target		✓
<a href="#">5.10</a>	Leveraging International Cooperation	---	---
<a href="#">5.11</a>	Norms of Behavior		✓
	<b>Enablers</b>	<b>United States</b>	<b>China</b>
<a href="#">5.12</a>	Enabling Laws		✓
<a href="#">5.13</a>	Domestic Surveillance		✓
<a href="#">5.14</a>	Civilian Institutions		✓
<a href="#">5.15</a>	Civilian IT Infrastructure		✓
	<b>TTPs</b>		
<a href="#">5.16</a>	Cyber in Gray-zone Applications		✓
<a href="#">5.17</a>	OCO as Elements of Complex Attacks		✓
<a href="#">5.18</a>	Vulnerability Mining		✓
<a href="#">5.19</a>	Leveraging Civilian Computers		✓
<a href="#">5.20</a>	Supply Chain Attacks		✓



UNCLASSIFIED

(U) With respect to the scale of Chinese cyber aggression towards the U.S., the conflict we find ourselves engaged in the information and cyber domains is frequently dismissed as a competition when it should be recognized as warfare. China doesn't hold the same perception of war and peace as the U.S. does. Examples supporting this contention are included throughout this document. Responding to cyber -enabled acts of war from a peacetime perspective keeps the U.S. at a disadvantage in terms of rules of engagement. It also projects weakness and a lack of resolve.<sup>197</sup>

UNCLASSIFIED

## 6.0 (U) Relative Abilities to Counter Cyber Threats

(U) Figure 3 on page 41 is a bar chart showing countries that host companies that reported cyberattack incidents as recorded in the online source KonBriefing.<sup>198</sup> Uncertainties associated with attribution and undetected cyber threats aside, one can draw some relevant observations from the data and make some meaningful inferences. First, when the data is segregated by NATO partner nations and traditional U.S. adversary nations, one observes that the average number of cyber attacks per year against NATO nations is close to twice the number reported against NATO adversaries. When only the top six nations ranked by the number of cyber attacks per year are considered for each group, the results are even more skewed with 943 attacks against the top six NATO countries and only 96 directed against the top six adversary countries. This is almost a 10:1 ratio of cyber aggression against NATO countries as opposed to NATO adversary nations.

(U) The probability of seeing this kind of bias in attack results if both groups were exposed to the same level of cyber threats would be about 0.021. Given the statistically significant result, one can conclude that the adversary nations, of which China is one, are more practiced at OCO's where the NATO partner nations have better opportunities to be more practiced at DCO's. One can extrapolate that those that are more practiced at OCO's will be more operationally effective at carrying out OCO techniques, developing and employing the requisite tools and engaging in the required training and management efforts. The same logic might be applied to DCO efforts, but one should consider that the processes by which one becomes more operationally effective in OCO's (e.g., vulnerability harvesting and exploitation tool development) will also yield information and tools that will enhance their own DCO stature.

(U) Reinforcing the notion that the U.S. is the biggest target worldwide for cyber aggression, the NCC Group Annual Threat Monitor for 2022 indicated that about 45.5% of the global cyberattacks were directed against the U.S. while only about 4% of them were directed against China. France was the next most targeted country with about 5.5% of the global cyberattacks.<sup>199</sup>

(U) The U.S. Senate report entitled "Federal Cybersecurity: America's Data Still at Risk" indicates that Chinese hackers "breached multiple Federal agencies" such that they could bypass passwords and multi-factor authentication and get to the agency's data. The same report indicated that according to the White House, over 30,819 information security incidents were recorded across the Federal Government in 2020.<sup>200</sup>

(U) Several high-profile attacks on the U.S. attributed to China are listed in an NSA/CISA/FBI cybersecurity advisory from 10/20/2020. They include: 1.) The Chinese military conducts a hack against the credit reporting service Equifax where trade secrets and the PII of tens of millions American citizens were impacted. 2.) a multi-year campaign of cybertheft of IP from 12 countries was reported in April of 2017. 3) In December of 2018 Chinese cyber threat actors were indicted for executing a large-scale phishing and spear-phishing campaign against Managed Service Providers as a means to steal business data and personnel PII. 4.) In May of 2020-the

FBI and CISA reported that cyber threat actors associated with China targeted and compromised U.S. organization involved with COVID-19 research.<sup>201</sup>

(U) A recent example of a large-scale cyberattack against U.S. government and commercial interests attributed to the PRC was reported on July 12<sup>th</sup>, 2023 in the New York Times Online periodical. Microsoft, who made the initial disclosure indicated that about 25 organizations, including government agencies, had been compromised by the hacking operation. The hackers used forged authentication tokens to get access to individual email accounts. It was determined that the attackers had access to some of the accounts for at least a month before the breach was detected. It was reported that no classified networks were impacted.<sup>202</sup>

### 6.1 (U) Cyber Connectedness and Dependencies

(U) As of 2020, 70.4 % of the population of China used the internet in some capacity.<sup>203</sup> Data from 2018, however, shows that about 98% of the 800 million internet users in China are accessing the internet through mobile devices- suggesting personal use as opposed to use associated with business, industry or government. That number would be closer to 16 million.<sup>204</sup> The majority of the 16 million non-mobile internet users in China are restricted to using Chinese websites, however, due to lack of English or other foreign language skills.<sup>205</sup>

(U) In contrast, 74% of the 241 million people (171 million) living in the U.S. owned a computer or laptop during the same period. These results suggest that the U.S. population would be more susceptible to making mistakes that would make them and the information systems that they use vulnerable to exploit.<sup>206,207,208</sup>

(U) A recent report from Verizon indicated that 82% of data breaches involved some element of human-induced vulnerability- or that only 18% of the breaches were accomplished through technical means alone.<sup>209</sup>

(U) The number of cyber-connected people in the U.S. creates an enormous attack surface and potential vectors for distributed and coordinated attacks. Human factors being the dominant component of data breaches has implications relevant to the comparative abilities of the U.S. and China to counter threats.

### 6.2 (U) Cyber Freedom and Information Controls

(U) The Chinese do not agree with the concept of an "open internet" and instead embrace the policy of "cyber sovereignty". The open internet standard of internet governance is a multi-stakeholder approach that the U.S. and many other countries embrace. These stakeholders work together towards an internet that is free, interoperable, and secure. However, with the multi-stakeholder approach, competing interests and lack of rigorous standards or standards enforcement come risks in terms of cyber defensive posture. The cyber sovereignty approach embraced by China places China in charge of its own related regulations, standards, rules of access and norms of conduct. Greater government control over the internet can and does translate to a more cohesive and consistent security posture in the case of China.<sup>210</sup>

(U) China's authoritarian regime overtly links information operations and cyber operations and executes tight control over them. One theory is that they fear the result of Chinese citizens

having free access to information. On the other hand, elements critical of the ruling political party in the U.S. still have some capability to have their messages heard, though in some cases, not without risk or serious ramifications including harassment, loss of employment, legal intervention or "cancellation".

(U) China controls how the Chinese-facing internet is used and what content is allowed to be seen. Chinese messaging to its population regularly refers to risks (imagined or real) posed by U.S. OCOs. Any such messaging by the any entities within the U.S. to its population is weak if it exists at all. If official messaging is a measure, Chinese citizens are probably more wary of opening suspect e-mails or clicking on links in malware than their American counterparts. This would represent an advantage for China over the U.S..

(U) In summary, China holds the defensive operational advantages of a smaller relevant attack surface and a population that is subject to government censorship, surveillance and messaging on matters relevant to cyber security.

### 6.3 (U) Attributes of Current Cyber Threats

(U) Chinese aligned cyber actors are skilled in adapting their tactics based on real-time surveillance of the cyber defender's actions. They will modify their tactics and toolsets essentially on-the-fly to respond to defensive actions.<sup>211</sup> When a cyber- attack has been identified, any offensive code can be isolated and characterized in terms of its size in bytes and its unique hash value. Using this data, the same offensive code can be searched for and found in other accounts and systems. The problem remains that it is easy for an attacker to make slight modifications to the code so the parameters are changed and security scans will not detect them.<sup>212</sup> Another tactic observed in Chinese aligned cyber threats is that they obscure their activities by embedding their exploitation tools within legitimate toolsets that would be expected to be found on a particular information system. This tactic aggravates the ability of defenders to identify a breach and allows the attack to remain undetected longer.<sup>213</sup>

(U) Automation is used as a force multiplier by cyber attackers. Mr. Michael Angelo, the Chief Security Architect at Micro Focus, indicated that "The methodology for attacking systems has been automated to the extent that a single entity can attack hundreds of thousands of machines in an hour."<sup>214</sup> In addition to being efficient, cyber threats (including those of the PRC) have proven to be resilient. The 2023 Global Threat report from CrowdStrike indicated that even when U.S. DCOs were successful and ransomware gangs were arrested and dismantled, that soon thereafter splinter groups emerged and flourished.<sup>215</sup>

(U) When it comes to matters of cyber warfare, it appears that advances in technology tend to favor the aggressor.

(U) With respect to Chinese defensive cyber operations, Winnona DeSombre, a research fellow at the Harvard Belfer Center testified before Congress that China's cyber defensive capabilities are able to "detect many U.S. cyber operations" and "in some cases are able to turn our own (offensive cyber) tools against us."<sup>216</sup>

#### 6.4 (U) Cyber Vulnerabilities

(U) In 2021, on average a new vulnerability was registered every 24 minutes.<sup>217</sup> The relatively recent emphasis on cloud networks, the Internet of Things (IOT) and AI has introduced new vulnerabilities to networks in the U.S. that tend to be thinly defended.<sup>218</sup>

(U) Robert Huber, the Chief Security Officer for Tenable, pointed out that there are "hundreds of software applications used in government agencies that introduce risk, and unpatched known vulnerabilities" - that are sources of data breaches.<sup>219</sup>

(U) Both offensive and defensive cyber capabilities rely on a robust ability to identify cyber vulnerabilities. Offensive cyber actors need vulnerabilities prior to being able to execute an attack. This fact represents an advantage in favor of China based on the Chinese industrialized approach to vulnerability detection.<sup>220</sup>

(U) Kristen Del Rosso, an incident response and threat intelligence product manager with Sophos compared the national vulnerability database of China (CNNVD) (maintained by the MSS) with the national vulnerability database of the U.S., which is maintained by the National Institutes of Standards and Technology. She found that the Chinese database contained about 196,000 vulnerabilities while the U.S. database contained about 12,000 less at 184,000.. Some of the vulnerabilities that the U.S. missed were considered particularly serious in that they were relevant to systems used in critical national infrastructure.<sup>221</sup>

(U) Consistent with Del Rosso's discovery, the news source Recorded Future reported that the U.S. national vulnerability database (NVD) is slower to include vulnerabilities after initial disclosure. They indicate that on average, it takes the U.S. NVD 33 days to include a vulnerability after initial discovery while it takes the CNNVD an average of only 13 days. They further indicate that 90% of vulnerabilities are captured within 18 days while it takes the NVD 92 days to cover the same percentage. Recorded Future attributes the tardiness of the NVD to the fact that it relies on the voluntary submission of data while CNNVD pulls data from extensive sources of vulnerability information across the web.<sup>222</sup>

(U) The U.S. and China have contrasting approaches to discovering vulnerabilities. As stated above, the U.S. relies on voluntary submission of vulnerabilities from industry, primarily. Reversinglabs assesses that the NVD is reflective of participation by a few large companies representing a handful of legacy platforms while open -source, newer technology and smaller companies are under-represented or choose not to participate at all.<sup>223</sup> On the other hand, China has adopted an incentivized approach. Chinese vulnerability reporters register with the CNNVD and then the rest of the process is similar to a game where the vulnerability reporters receive status, incentives and engage in competitions.<sup>224</sup>

(U) As an objective measure, the PRC's ability to outperform the U.S. in vulnerability discovery suggests that at least at that time, the PRC was better at finding and reporting vulnerabilities than the U.S. Recorded Future adds "While the U.S. government has focused on a process, China has focused on the key goal — quickly reporting available vulnerabilities."<sup>225</sup>

## 6.5 (U) Contrasting DCO Approaches

(U) In an address to the Army War College 2021 graduating class, Deputy Secretary of Defense, Kathleen Hicks characterized the U.S. ability to pursue common economic and security goals with other nations through alliances and partnerships as an asymmetric advantage that the U.S. has over adversaries (such as China).<sup>226</sup> An article relating to a cyberattack on the Albanian government by Iran included a quote from MG William Hartman, CDR US Cyber National Mission Force. CDR Hartman indicated that "hunt forward" cyber teams are key enablers of US cyber- force's ability to uncover "new data and information about the tools, techniques and procedures of malicious cyber actors."<sup>227</sup>

(U) While the motivations might differ with respect to a country's willingness to cooperate with American or Chinese cybersecurity interests, it seems evident that bribery, coercion and economic pressure will remain as effective tools for gaining cooperation from international entities.

(U) Zero-trust information security architectures provide improved security by effectively setting up authentication gateways, including multi-factor authentication, in order to deny or restrict an intruder's mobility in the event that the intruder gains access to a protected asset. In effect, the system will make no assumptions about the identity and access privileges of a user- it will require independent authentication at every stage of interaction with the IT system. The U.S. Defense Information Systems Agency (DISA) completed its new zero-trust network access architecture that it refers to as "Thunderdome". Through its zero-trust approach, Thunderdome is expected to ensure that only the right people are able to access the right data, on a managed device, from a trusted location at appropriate times.<sup>228</sup>

(U) In the face of increased cyber aggression from the PRC against the U.S. and non-cyber diplomatic, economic and geo-expansionist pressures and general tension over the fate of Taiwan, the U.S. Department of Justice (DOJ) scrapped its "China Initiative" that was engaged under the Trump administration, in 2022. The China Initiative focused on national and criminal threats posed by China. Reasons cited by the DOJ included that the China Initiative sapped resources that could be directed against increasing threats posed by Russia and Iran, for example. They also expressed concern over the potential for increased hate crimes against persons of Asian descent. The civil rights community in the U.S. complained that the DOJ's investigations into Chinese cyber espionage against the U.S. "unfairly" targeted "academics of Asian descent". A DOJ spokesperson reiterated this notion remarking that "erosion of trust in the department can impair our national security. It alienates us from the people we serve..."<sup>229</sup>

(U) Avoiding large-scale investigations into large-scale Chinese cyberespionage and cybercrime enterprises because China is not the only entity engaged in the nefarious practices or because of a fear that the U.S. population will lash out against innocent Asian citizens or because the perpetrators of the crimes are Asian (i.e., Chinese), does not appear to be a robust legal foundation for countering cyberattacks by China. In light of China's clear and concerted efforts to prioritize and reinforce its cybersecurity posture with laws, government policy and cyber

operations, the contrasting mindsets and governing approaches between the U.S. and the PRC should be considered an advantage in favor of the PRC.

(U) The National Security Division of the U.S. DOJ is involved with pro-active cyber defense such as detecting and neutralizing botnets.<sup>230</sup> They also engage in deterrence activities. Cyber deterrence at the hands of DOJ takes on the form of enforcing sanctions and export controls; mitigating cyber risks due to foreign investment and investigating and charging cases of cyber-crime by foreign nationals.<sup>231</sup>

(U) Former NSA Director Mike Rogers indicated that there is consideration in the U.S. of making ransom payments in response to ransomware attacks illegal in the U.S.. The government of Australia is also considering making the ransom payments illegal.<sup>232</sup> An article dated November of 2022 indicated that the Defense Intelligence Agency (DIA) was planning on standing up a China Mission Group to monitor the growing cyber threat posed by China. The China Mission Group will function as DIA's repository for knowledge, know-how and "deep expertise." The China Mission Group is expected to be established in early 2023.<sup>233</sup> An observer might consider the vast number of Chinese cyber- attacks against the U.S. beginning in about 2018 as evidence that China has had some kind of "U.S. Mission Group" at the highest levels of their military and state security organizations for some time. That the U.S. is just now considering whether to ban ransomware payments and setting up such a program like the "China Mission Group" within a key intelligence agency can be considered a measure of its cyber defense readiness relative to that of the PRC's.

(U) The governments of the U.S., EU, UK and Canada have all banned the use of the TikTok app on government equipment based on the risk that the devices themselves could be used to spread Chinese propaganda and misinformation or send information and communications to Chinese servers. While the TikTok app might be worthy of being banned from government systems. It is one of many apps in use on government computers that may be posing active security risks.<sup>234</sup> In 2019, prior to the TikTok controversy, the PRC ordered the phase out of all foreign network hardware and software from its government offices and public institutions within 3 years. Consequently, the PRC would appear to be in a more robust cybersecurity posture with respect to risks posed by foreign hardware and software.<sup>235</sup>

(U) The PRC has gained itself an advantage in its ability to counter threats by virtue of their efforts to depart from global IT standards and protocols in favor of domestically produced ones. One can expect that it would be harder to scan for vulnerabilities, produce effective offensive tools, and execute cyberattacks against Chinese systems that are not conformal to global standards and protocols.<sup>236</sup> Under a policy of universally observed standards (as embraced by the U.S.) offensive cyber tools and techniques would be applicable against any potential foe. China moving away from the universal standards complicates and raises the cost of OCOs against PRC assets. PRC independence from Western technology can be expected to lead to an advantage for the PRC in terms of the detection of vulnerabilities and interoperability of exploits. Technology development in the PRC will be less exposed to entities outside of the control of the CCP and therefore less vulnerable. Distancing themselves from universal IT-related standards



can also be expected to make the Chinese more robust against supply chain attacks in comparison with the U.S. which uses universal IT standards.

(U) With respect to advanced microchip production, there are efforts to enhance the domestic capability to produce microchips in the U.S., which is a positive development for the U.S.<sup>6</sup> While the U.S. currently relies on Taiwan for advanced microchip fabrication, the PRC is rapidly developing their domestic capability to produce mature and high-end chips. Development of a Chinese microchip manufacturing capability is in the context of the "de-Westernization" of the technology supply chains in the PRC.<sup>237</sup> The resulting independence from Taiwanese and other advanced semiconductor markets in east Asia will provide the PRC an advantage over the U.S. in terms of resiliency to cybersecurity-related supply chain attacks as well as an enhanced ability to field new and replacement cyber-enabling hardware.

(U) The bottom line is that U.S. systems will remain more vulnerable based in part on the openness of the technology in the international arena. Chinese technology, presuming that it remains under the control of the CCP can be considered to be harder to exploit based on the closed nature of their technology.

#### 6.6 (U) Defending Against "Botnets"

(U) "Botnet" is a term for a network of infected computers that can be commanded to execute malicious functions as an orchestrated group. The problem of botnets for DoD is particularly vexing because the majority of botnet nodes lie outside of the DoD global information grid.<sup>238</sup> In 2019, while discussing their Harnessing Autonomy for Countering Cyberadversary Systems (HACCS) initiative, DARPA officials indicated that current incident response methods (as applied to botnet threats) were too resource dependent and time consuming to address the problem at scale.<sup>239</sup> Active defense methods against botnet attacks are themselves risky and their effects on proper system function are hard to predict.<sup>240</sup>

(U) The relative risk of botnet attacks is slanted toward the U.S. and away from the PRC. This is because more Americans use computers for personal and home business and for entertainment. Americans are a more cyber-connected society. We also have great autonomy to access any web destinations that we see fit without restrictions. We have no overarching web authority policing our actions in cyberspace. The relative freedom in the U.S. allows American citizens to expose themselves either wittingly or unwittingly to more risks than a censored and tightly cyber-regulated society like China does.

#### 6.7 (U) Cybersecurity System Patches

(U) Previously in this report we describe the Chinese culture as being constrained in terms of websites they can access and software they can run. We also made the point that the vast number of Chinese citizens don't typically employ connected devices for other than smartphone applications and communication. American culture is in stark contrast to Chinese culture in this

---

<sup>6</sup> (U) 75% of global microchip production takes place in East Asia and 90% of the most advanced chips are made in Taiwan. Only about 10% of computer chips are produced in the U.S. (Barnes, J.. "How the Computer Chip Shortage Could Incite a U.S. Conflict With China". New York Times Online. Web Article. 1/26/2022.)

way. For the Chinese, fewer cybersecurity patches are necessary, they are easier to administer, and the Chinese likely find out about the vulnerability sooner and the overall vulnerability surface is smaller.

(U) Clearly, cybersecurity patching is more critical to the U.S. based on the vastly greater number of cyberattacks that the U.S. is subject to in comparison with the PRC.

(U) Cybersecurity patches are only directly relevant to known vulnerabilities. Data from January of 2018 through September of 2019, collected by the cybersecurity firm Mandiant showed that 42% of vulnerabilities were exploited after a patch was made available with the balance being exploited as zero-day vulnerabilities.<sup>241</sup> This indicates that cybersecurity patches are relevant to about 40% of attacks based on exploited vulnerabilities. It also shows that network administrators are failing to a large extent, to patch their systems.

(U) The Mandiant report also states that it takes an average of 9 days before a patch is made available after a vulnerability is discovered.<sup>242</sup> Naturally it would be advantageous to the U.S. to reduce this window of vulnerability. Based on the Mandiant sample, 38% of exploits could have been avoided if available patches were applied in a timely manner.<sup>243</sup>

(U) A cybersecurity advisory issued by the CISA in 2022 indicated that network and data infrastructure devices are often left vulnerable while cyber defenders struggle to keep pace with software patching processes required for their internet-facing and endpoint service systems.<sup>244</sup>

(U) The Mandiant study also showed that 12% of exploits occurred more than two months after a patch was available.<sup>245</sup>

(U) Once an exploit is successful and an IT system is penetrated, the dwell time metric becomes operative. Dwell time is the time of intrusion through the victim being aware of the intrusion. Mandiant collected data on dwell time and they reported that global median dwell time is improving with a median time for intrusion detection of 3 weeks. No comparable statistics for Chinese networks were available in the literature.<sup>246</sup>

(U) To put these timeframes in context, in 2022 the cybersecurity firm Crowdstrike measured the average time that it took an attacker to move from one exploited host to another host as 84 minutes. Crowdstrike advocates for the "1-10-60 rule" for cybersecurity teams. The rule specifies that a cyberthreat should be detected within one minute; understood within 10 minutes and responded to within 60 minutes.<sup>247</sup>

## 6.8 (U) Defensive Cybersecurity Posture and Priority

(U) While zero-day vulnerabilities are highly prized by hackers and are of key importance to network and data defenders, the top 20 list of the most commonly exploited vulnerabilities used by Chinese supported threats (as reported by NSA and CISA in a 10/6/2022 Cybersecurity Advisory) comprises previously known and patchable vulnerabilities. About 85% of the top 20 list were vulnerabilities that were more than a year old.<sup>248</sup>

(U) The poor performance of network professionals in ensuring that their systems are patched suggests either a lack of motivation, skills, training, controls or processes that they need to

routinely check and patch their systems. It is also possible that some individuals trusted with stewardship of networks and data have been seduced by easy money to allow their systems to remain unpatched and vulnerable to exploits by cyber threat actors. Another factor is an insufficient number of trained, skilled and experienced cybersecurity professionals. The PRC has energetic programs and pipelines from its universities, industries and hacker communities to engage new cybersecurity professionals at the forefront of the cybersecurity efforts of its military and security agencies. The SSF are an example of one of these pipelines. In contrast, according to the 2022 Global Threat Report by CrowdStrike, cyber security teams in the U.S. were strained in 2021 and that there is an ongoing cybersecurity skills shortage. There are no indications in the literature that the PRC is experiencing a similar shortage of cyber professionals supporting OCOs and DCOs for the PRC.<sup>249</sup>

(U) In June of 2019 a U.S. Senate subcommittee issued a report that found that eight key federal agencies failed to comply with basic Federal cybersecurity standards and protocols. The gaps in security left the personally identifiable information (PII) of Americans unprotected and included the failure to promptly install security patches – leaving systems vulnerable to exploit. Two years later the same 8 agencies were revisited and re-evaluated and all but one made nothing but minimal improvements such that the information systems and the sensitive data that they store remained at risk.<sup>250</sup>

(U) The UCESRC assesses that the U.S. will face a formidable challenge in defending against China's daily cyber intrusions and in defending against China's OCOs should a high-end conflict break out.<sup>251</sup> The UCESRC indicated that "Urgent questions remain concerning the United States' readiness for the China cyber challenge." These questions relate to: 1.) the adequacy of resourcing for U.S. military cyber forces; 2.) the sufficiency of existing protections for U.S. critical infrastructure, and 3.) the scope of public-private cybersecurity cooperation.<sup>252</sup>

(U) The NSA/CISA/FBI cybersecurity advisory of 7/19/2021 assessed that the Chinese state-sponsored cyber actors use a "full array" of tactics and techniques to exploit computer networks and to acquire sensitive IP and economic, political and military information. This assessment from the highest levels of the American cybersecurity operational community suggests that the Chinese OCOs remain a serious challenge to the U.S..<sup>253</sup> Winnona DeSombre, a research fellow at the Harvard Belfer Center testified to Congress in March of 2022 that China has earned cyber-peer status with the U.S. by virtue of their demonstrated ability to successfully compromise U.S. targets and their ability to detect some U.S. state-sponsored cyber operations. She assessed at the time that the U.S. did not have adequate cyber defenses, personnel, or supply chain security to "rival China long-term in cyberspace."<sup>254</sup>

(U) Chinese Communist Party and General Secretary and leader of the government, Xi Jinping has made very clear the high priority that he places on cyber capability and dominance. He has been quoted as saying "the Internet is at the forefront of the current ideological struggle". He directed his subordinates to maintain "online ideological security." He has also stated that a country's ability to master the internet determines its rise or fall and that "those who win the internet win the world."<sup>255</sup> The General Secretaries high priority on cyber dominance appears to

be reflected in every relevant aspect of Chinese culture and is reflected in all of the Chinese major institutions.

(U) While the U.S. might have the technology and expertise on hand to secure their information infrastructure, they might lack the will, motivation or leadership to do so. This would be in stark contrast to the Chinese who are working to be cyber-dominant. The amount of emphasis placed on cybersecurity relative to other issues of state including the climate change, energy policy, inclusivity and the threats posed by domestic extremists appears to be an area of contrast between the current leadership of the U.S. and China.

(U) The U.S. Senate report entitled "Federal Cybersecurity: America's Data Still at Risk" indicates that Chinese hackers "breached multiple Federal agencies" such that they could bypass passwords and multi-factor authentication and get to the agency's data. The same report indicated that according to the White House, over 30,819 information security incidents were recorded across the Federal Government in 2020.<sup>256</sup> After 30,819 cyber attacks and a failing grade in cybersecurity, one would expect the U.S. Government (USG) to pay more attention to its cybersecurity stature.<sup>257</sup>

(U) Ian Bremmer, the founder and president of the Eurasia Group assessed that "America's greatest vulnerability is its continued inability to acknowledge the extent of its adversary's capabilities when it comes to cyber threats."<sup>258</sup> It is clear that the critical importance of cybersecurity is not lost on General Secretary Xi Jinping .

## 6.9 (U) Conclusions

(U) This chapter identified several factors that are a basis of distinction between U.S. and Chinese defensive cyber capabilities and readiness.

(U) Table 3 lists the factors addressed in this chapter together along with columns indicating whether an advantage is held by either the U.S. or the PRC in terms of each factor. A dashed line indicates that no advantage is realized and a check indicates whether an advantage exists and which country enjoys the benefit. The assessments in the table are from the analyst and are based mainly on a review of open-source materials. Supporting discussions are in the relevant sections of this chapter.

*(U) Table 3 Factors Impacting the Defensive Cyber Capabilities of a State Cyber Force*

UNCLASSIFIED		UNCLASSIFIED	
Section	Factor Contributing to Defensive Cyber Capability	Advantage of State Cyber Force based on Contributing Factor	
	Strategic Approach	United States	China
<a href="#">6.0</a>	Practiced at Defensive Cyber Operations (based on volume of attacks)	✓	
<a href="#">6.1</a>	Smaller Vulnerability Surface		✓
<a href="#">6.2</a>	Cyber Freedom and Information Controls		✓
<a href="#">6.3</a>	Technology Favoring the Aggressor		✓
<a href="#">6.4</a>	Vulnerability Exploitation		✓
<a href="#">6.5</a>	Independence from Dominant IT Standards		✓
<a href="#">6.5</a>	Robust against Microchip Supply Chain Attacks		✓
<a href="#">6.7</a>	Cybersecurity Patches		✓

(U) There are attributes of the U.S. culture that no American would want to depart from. These include the aspects of cyber-freedom and freedom of information flow. Americans will not want to depart from the conveniences and capabilities that internet connectiveness provides. Nonetheless, these attributes are associated with increased susceptibilities to human error, increased reliance on human performance and an all-around increase in vulnerability and a diminished capability to defend vital assets. For this matter, the USG needs to increase the priority that they currently place on cybersecurity across the spectrum of government authority. The priorities should be emphasized in a public manner so the general population is aware of the risks associated with national subjugation in the cyber domain. Leadership needs to be clear and actions recognizable as necessary to defend against a current and immediate existential threat to our nation. Messaging about cybersecurity priorities, like other national security priorities should not be muddled or confused with, or diminished by messaging about political, cultural or otherwise, non-existential issues of the day.

## 7.0 (U) Recommendations to Improve the Cybersecurity Posture of the U.S.

(U) A theme that tended to recur throughout the review of literature and within this paper is that the PRC holds several advantages over the U.S. in terms of cybersecurity. Many of the advantages are rooted in disparate values maintained by the two countries. Some are based on militaristic priorities that have been fully embraced by the authoritative leaders of the CCP and President Xi Jinping. These priorities have been imposed on the Chinese people at the cost of many freedoms that many Americans take for granted- and which most Chinese citizens have never known. Regardless, the review of the literature resulted in several measures that could be implemented that could be expected to improve the cybersecurity posture of the U.S.. These measures are described in the following subsections. The subsections are not presented in any prioritized order.

### 7.1 (U) Continue to Emphasize Zero-Trust Architectures and Multi-Factor Authentication

(U) The 2023 Global Threat Report by CrowdStrike recommends a continued emphasis on Zero-Trust architectures and multi-factor authentication for enhanced cybersecurity postures. They caution against underestimating the risk of human error and of social-engineered phishing attacks. Legitimate log-in credentials are a big business for hackers and attempts to collect log-in credentials using sophisticated social engineering attacks involving e-mails, text messages and phone calls (as opposed to just clicking on a link in an e-mail) are becoming common.<sup>259</sup>

### 7.2 (U) Raising Awareness and Improving Cybersecurity Education

(U) Amazon and the National Cybersecurity Alliance have recognized the core issue aggravating the cybersecurity posture of the United States. This is "tens of millions of technologically unsavvy Americans". These Americans will continue to pose cybersecurity risks as they continue to fall for phishing scams; keep their anti-virus capabilities and home computers up to date. At work, these Americans are weak links in their employer's network security. Cybersecurity education programs are necessary in order to address and mitigate this risk area.<sup>260</sup> Human beings are the core enabling vulnerability and common denominator for most cyberattacks. Human beings can be tricked, bought-off, lazy, or simply make an honest mistake that can lead to a costly cyberattack. Compromised employees allow attackers to bypass significant portions of an organizations defensive controls, and the humans cannot be "patched". Going forward, cyber security education and training efforts need to be supplemented operational tests and drills in order for people to understand the risks, consequences and what a robust cybersecurity posture feels like. Cyber drills can be framed like fire drills and "See something- Say something" games or challenges in cyberspace.<sup>261</sup>

(U) Consistent with Chinese military textbooks, many experts on China assess that the PLA has been preparing a major cyberattack on the US for decades.<sup>262</sup> Chinese President Xi Jinping has stated on multiple occasions that "Cybersecurity is, ultimately, a competition for talent." U.S. policy makers should consider that wisdom and enhance their efforts to invigorate the U.S.'s cybersecurity education and research pipeline and ultimately attract talent from abroad.<sup>263</sup>

(U) An important enabler for improving cybersecurity awareness and education is to embrace a policy of open discussion about the vital issue. The population needs to be informed about the well-crafted plans and current capabilities to attack their vital information infrastructure. The U.S. engaged in civil defense drills and participated in multimedia tests of civilian-directed emergency response systems. These efforts, which were started in the mid 20th century have since been abandoned as if the U.S. no longer faces any threats. Newer versions of them would be important steps towards preventing panic and social upheaval in the event of a large-scale cyberattack on civilian infrastructure.

### 7.3 (U) Survey Chinese-sourced Network Technology and Perform a Risk Assessments

(U) The U.S. should catalog Chinese -sourced technology such as surveillance systems, operational technology, and other infrastructure-bound technologies and assess the risks that they might pose based on their placement and application and the potential that malicious code or functions could be activated.<sup>264</sup>

### 7.4 (U) Engagement with Domestic Hacker Community

(U) The U.S. Government should work to emulate the positive aspects of the relationship that the Chinese government enjoys with its cybersecurity/ hacker community. The USG should foster the notion that cybersecurity experts and hackers can and do play a vital role in national security. Further, the USG should encourage positive relationships between industry and the hacker community.

### 7.5 (U) Make Optimal Use of the Department of Commerce Entity List

(U) Chinese universities that are known to engage in cyber-related research on behalf of the Chinese government should be entered on the U.S. Department of Commerce's (DOC) Entity List. While adding the universities to the entity list will not impact the school's ability to conduct cyber research for the government, it will prevent other departments within the universities from accessing American talent and resources.<sup>265</sup> The existence, purpose and importance of the DOC Entity List needs to be fully communicated to the relevant audiences.

### 7.6 (U) Pre-Emptively Engage with Wider International Audience on Cybersecurity

(U) The U.S. should work to improve regional cyberdefense capabilities and cooperation among Asian countries that themselves are frequently targeted by PRC OCOs. Current tensions in the Asia-Pacific region could provide a basis for closer cooperation that was possible in the past. The cooperation could lead to identification of PRC tools, tactics and procedures that could benefit our own cyber defense at critical times.<sup>266</sup>

### 7.7 (U) Improve Domestic Vulnerability Detection Process

(U) The U.S. should emulate the Chinese approach to vulnerability detection and reporting processes, especially in terms of incentives and streamlined inclusion to the U.S. NVD.<sup>267</sup>



### 7.8 (U) Enhance Code Supply Chain Security

(U) U.S. cybersecurity authorities need to pay close attention to supply chain attacks on code modules, firmware and updates and investigate ways to make these processes more secure.

### 7.9 (U) Make a Cybersecurity Common Operational Picture Available to Wider U.S. Cybersecurity Stakeholder Community.

(U) The U.S. needs an integrated and coherent Common Operating Picture (COP) available to all information system stakeholders (i.e., Government, industry and academia) that will show adversary actions in the cyber domain. The report by Nissen, et al states succinctly, "We live in an asymmetric era in which dominance is won through non-kinetic exploitation of open societies." While there are expert cybersecurity surveillance assets at work in the public and private sector, we still lack an integrated repository of that data that is updated in operationally relevant timeframes.<sup>268</sup>

### 7.10 (U) Enable Some Private Sector OCO's and DCO's

(U) Contrary to Chinese Law, which requires that Chinese business and industry cooperate with the Chinese military intelligence apparatus on matters concerning operations in cyberspace and information operations<sup>269,270</sup>, American companies are legally prevented from taking anything but strictly defensive measures to protect their information assets. In the U.S. most of our military and commercial IP originates or resides in the private sector and as a result, private sector entities find themselves on the front lines facing state-backed APTs or proxies for the Chinese military in the Chinese business sector. The U.S. and her private sector should work together towards a more robust cybersecurity and cyber-deterrence posture.<sup>271</sup> The U.S. and her private sector should embark on a government/industry partnership approach to cyber defense and response, to include DCO as well as OCO. The partnership should include intelligence sharing; developing and exercising cyber-response playbooks; and developing and employing pre-defined countermeasures. Rules of engagement need to be refined that will make the cost of engaging in OCO against the U.S. a deterrent factor.<sup>272</sup>

### 7.11 (U) Emphasize Cyber S&T Efforts that would leverage AI

(U) Tools that automatically scan for vulnerabilities for OCO or DCO purposes will be key in the ability to mitigate or respond to large scale cyberattacks and cyberattack risks. S&T efforts should focus on these types of tools.

### 7.12 (U) Move Toward Closed IT Standards for Critical Applications

(U) There are no cybersecurity benefits to using widely understood IT standards and no IT system ever became more secure by ensuring that it's communication protocols and security features were widely known. There are likely some applications where adopting closed standards would be practicable and would be associated with improved security posture. Efforts should be made to identify these applications and to move toward developing and implementing new, closed IT standards and protocols to be used in military and sensitive government networks. SCADA and operational technology systems for vital infrastructure should also be protected with a newer, more secure set of closed standards.

#### 7.13 (U) Improve Communication on OCO Justification

(U) If OCOs can be justified, the basis of their justification should be established up front and readily communicatable. Concepts of scaled severity similar to how the terms "misdemeanor" and "felony" relate to crimes could be used to provide more clarity to cyber-related infractions. The distinction between what constitutes a nuisance act; a cyber-crime; or, an act of cyberwar should be established and publicized. Publicly acknowledging employees that effectively employ good cybersecurity -risk discernment skills could be among the ways the human vulnerability surface can be reduced.

#### 7.14 (U) Build Trust and Earn Back Cyber-Credibility

(U) In order to regain some degree of credibility and to shore up a leadership role on the international stage of cyberspace norms of behavior, the U.S. will have to be communicate more clearly and effectively about what OCO's are acceptable based on target type, and prevailing circumstances. The appearance that the U.S. operates beyond the norms of behavior that it prescribes to the rest of the world must be corrected. It needs to establish that not every OCO that it engages in is a violation of the rules for cyberspace that it is proposing.

### (U) Acronyms

## UNCLASSIFIED

UNCLASSIFIED	UNCLASSIFIED
5G	5th generation (telecommunication protocol)
ADM	Admiral
AI	Artificial Intelligence
APT	Advanced Persistent Threat
ATW	Against the West
BGP	Border Gateway Protocol
BRICS	Brazil, Russia, India, China and South Africa
CCP	Chinese Communist Party
CERT-FR	Cybersecurity Emergency Response Team- France
CIA	Central Intelligence Agency
CISA	Cybersecurity and Infrastructure Security Agency
DARPA	Defense Advanced Research Projects Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIB	Defense Industrial Base
DIR	Director
DISA	Defense Information Systems Agency
DOC	Department of Commerce
DoD	Department of Defense
DODIN	Department of Defense Information Network
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FOCAC	Forum on China-Africa Cooperation
FY	Fiscal Year
GIS	Geographic Information System
H4D	Hacking for Defense
HACC	Harnessing Autonomy for Countering Cyberadversary
IC	Intelligence Community
ICT	Information and Communication technology
IDA	Institute for Defense Analysis
IISS	International Institute for Strategic Studies
IO	Information Operation
iOS	(Apple smartphone operating system)
IOT	Internet of Things
IP	Intellectual Property
ISP	Internet Service Provider
IT	Information Technology

## UNCLASSIFIED

JWICS	Joint Worldwide Intelligence Communication System
MIIT	Ministry for Industry and Information Technology
MITM	Man in the Middle
ML	Machine Learning
MOOTW	Military Operations Other Than War
MSS	Ministry of State Security
NATO	North Atlantic Treaty Organization
NCC	National Computing Centre
NDAA	National Defense Authorization Act
NDU	National Defense University
NIST	National Institute of Science and Technology
NSA	National Security Agency
OCO	Offensive Cyber Operations
OPM	Office of Personnel Management
OUSD(R&E)	Office of the Under Secretary of Defense for Research and Engineering
PII	Personally Identifiable Information
PLA	Peoples Liberation Army
POC	Proof of Concept
PRC	Peoples Republic of China
QKD	Quantum Key Distribution
R&D	Research and Development
RSA	Rivest, Shamir and Adleman
S&T	Science and Technology
SASTIND	State Administration of Science Technology and Industry for National Defense
SCADA	Supervisory Control and Data Acquisition
SIPR	Secure Internet Protocol Router
SMOKE	Signature Management Using Operational Knowledge and Environments
SSF	Strategic Support Force
TRB	Technical Reconnaissance Bureau
TTPs	Techniques, Tactics and Procedures
UCESRC	U.S.-China Economic and Security Review Commission
USG	U.S. Government

## (U) References

(All references are Unclassified)

---

<sup>1</sup> Kamphausen, R.. "Modernizing Deterrence: How China Coerces, Compels and Deters". National Bureau of Asian Research. Report. 2023. P 10

<sup>2</sup> Wang Z., Yangyue, L., "Analysis of Strategies for Interactions in Cybersecurity", National Defense Technology 42, no. 5. Article. 2021. (as referenced in Beauchamp-Mustafaga, N., Kamphausen, R.. "Modernizing Deterrence: How China Coerces, Compels and Deters". National Bureau of Asian Research. Report. 2023. P 126

<sup>3</sup> Zhengrong, C., Renbo, W. and Jianjun, S.. "Informationized Joint Operations". People's Liberation Army Press, Beijing, China. Textbook. 2006, Chapter 2. Referenced in Hodgeson, Q., (et al), "Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace." RAND. Report. 2019. P 18

<sup>4</sup> Tarabay, J., Wang, C.. "Taiwan Rushes to Prevent China From Cutting Off Internet, Phones". Bloomberg News. Article. 5/29/2023.

<sup>5</sup> Periroth, N., "How China Transformed Into a Prime Cyber Threat to the U.S.". New York Times. Article. 7/20/2021.

<sup>6</sup> Alspach, K.. "Russian Hackers get the Headlines. But China is the bigger threat to many US Enterprises.". Protocol. Article. 8/3/2022.

<sup>7</sup> Alspach, K..

<sup>8</sup> Raud, M., "China and Cyber: Attitudes, Strategies, Organization". NATO Cooperative Cyber Defence Centre of Excellence. Report. 10/10/2016. P 6, 24

<sup>9</sup> "APT1: Exposing One of China's Cyber Espionage Units". Mandiant. Report. 9/13/2021. P 9

<sup>10</sup> Cheng, D. "China's Quest for Information Dominance". Association of Old Crows. Podcast "From the Crows Nest". 4/26/2023.

<sup>11</sup> Aitel, D., d'Antoine, S., Bulazel, A., DeSombre, W., Garcia-Camargo, I., Garwin, T., Roos, I., Rostow, N., Wagner, A.. "China's Cyber Operations: The Rising Threat to American Security". Margin Research. Paper. 2022. P 2

<sup>12</sup> "2023 Cybersecurity Almanac". Momentum Cyber. Report. 2/22/2023. P 9.

<sup>13</sup> "2022 Report to Congress". U.S. China Economic and Security Review Commission. Report. 11/2022. P 435, 436

<sup>14</sup> Harold, S., Libick, M., Cevallos, A.. "Getting to Yes with China in Cyberspace". Rand Corporation. Report. 2016. P 30

<sup>15</sup> "2022 Report to Congress". U.S. China Economic and Security Review Commission, P 447

<sup>16</sup> Raud, M., P 24

<sup>17</sup> Houqing, W.and Xingye, Z.."The Science of Military Campaigns". National Defense University Press, Beijing, China. Textbook: 2000, pp. 173–174, referenced in Hodgeson, Q., (et al), "Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace." RAND. Report. 2019. P 18

<sup>18</sup> Nissen, C., Clancy, C., Ledgett, R., Sledjeski, C. " Beyond Solarwinds: Principles for Securing Software Supply Chains". MITRE Corp. Report 21-0843. 3/18/2021. P 3

<sup>19</sup> Kamphausen, R., P 9

<sup>20</sup> "U.S. Intel Officials Detail Threats From China, Russia". U.S. STRATCOM DOD News. Article. 3/8/2022. P 3

<sup>21</sup> Liu, N.. "China's Strategic Support Force Brings Hybrid Warfare to Space, Cyber, Politics". Voice of America. Article. 3/21/2023. P 1

<sup>22</sup> Williams, B. K.. "Evaluating China's Road to Cyber Super Power". Lawrence Livermore National Laboratory, LLNL-TR-829221. Report. 11/15/2021. P 8

<sup>23</sup> Liu, N., P 3

<sup>24</sup> Beauchamp-Mustafaga, N., Kamphausen, R.."Modernizing Deterrence: How China Coerces, Compels and Deters". National Bureau of Asian Research. Report. 2023. P 126

<sup>25</sup> Kamphausen, R., P 108

<sup>26</sup> Wenxian, Y.. "Lectures on Joint Campaign Information Operations". Military Science Press, Beijing, China. Textbook, 2009, p. 109. Referenced in Hodgeson, Q., (et al), "Fighting Shadows in the Dark: Understanding and Countering Coercion in Cyberspace." RAND. Report. 2019. P 18

<sup>27</sup> Goswami, R., “Chinese state-sponsored hackers infiltrated U.S. naval infrastructure, Secretary of the Navy says”. CNBC.com. Web Article. 5/25/2023.

<sup>28</sup> Harold, S., Libick, M., Cevallos, A.,P xii

<sup>29</sup> Jili, Bulelani. "China's Surveillance ecosystem and the global spread of its tools". Issue Brief. Atlantic Council. 10/17/2022. P4.

---

<sup>30</sup> Jili, Bulelani. P4.

<sup>31</sup> Bowman, J.. "A Modern Great Wall: PRC Smart Cities and the A2/AD Implications for AFSOC". Naval Postgraduate School. Thesis. 6/2022. P 40

<sup>32</sup> "2022 Global Threat Report". Crowdstrike. Report. 9/28/2022. P 3

<sup>33</sup> Aitel, D., d'Antoine, S., Bulazel, A., DeSombre, W., Garcia-Camargo, I., Garwin, T., Roos, I., Rostow, N., Wagner, A.. "China's Cyber Operations: The Rising Threat to American Security". Margin Research. Paper. 2022. P 4

<sup>34</sup> "Strategic Support Force Recruitment in the Central Theater Command: Unit 32081 and the Technical Reconnaissance Base". Crowdstrike. Intelligence Report. 2023. P 4

<sup>35</sup> Pomerleau, M. "DOD unveils cyber workforce implementation plan, taking a 'different approach' to managing talent". DefenseScoop.com. Article. 8/3/2023

<sup>36</sup> "About the Course- Hacking for Defense". BMNT and the Common Mission Project. Web page. URL: <https://www.h4d.us/about-h4d>. Accessed: 8/29/2023

<sup>37</sup> Work, J.D.. "China Flaunts its Offensive Cyber Power". War On The Rocks. Texas National Security Review. Article. 10/22/2021. P 14-15

<sup>38</sup> MacGhillionn, J.. "China's Cyber Capabilities Pose and Existential Threat to America". The Epoch Times. Article. 2/13/2022. P 7.

<sup>39</sup> "International Cybersecurity Contest". Web page. Tianfu Cup. URL: <https://www.tianfucup.com/2022/en/index>. Accessed: 3/31/2023

<sup>40</sup> Tarabay, Jamie." China Shows Its Hacking Prowess at \$2 Million Contest". Bloomberg News. Article. 10/29/2021. URL: <https://www.bloomberg.com/news/newsletters/2021-10-29/china-shows-its-hacking-prowess-at-2-million-contest>.

<sup>41</sup> Work, J.D.. P 11.

<sup>42</sup> "Tianfu Cup 2021 - Windows 10, Chrome, iOS, Linux Exploited". Defense Lead. Article. 10/20/2021

<sup>43</sup> Work, J.D.. P 7.

<sup>44</sup> Work, J.D.. P 4.

<sup>45</sup> Jili, Bulelani.. P4.

<sup>46</sup> Work, J.D... P 14-15



- 
- <sup>47</sup> Cary, D.. "Dakota Cary's Testimony Before the U.S.- China Economic and Security Commission". UCESC. Testimony. 2/17/2022. P 4
- <sup>48</sup> Jili, Bulelani.. P4.
- <sup>49</sup> O'Neill, P.. " How China Built a One-of-a-Kind Cyber-Espionage Behemoth to Last". MIT Technology Review. Article. 2/28/2022. P 4
- <sup>50</sup> O'Neill, P.. P 5
- <sup>51</sup> DoD EW COI meeting 5/8/2023. Meeting Summary. 5/10/2023
- <sup>52</sup> "The Chinese Private Sector Cyber Landscape".. Margin Research. Paper. 4/25/2023. P 2
- <sup>53</sup> "2022 Report to Congress". U.S. China Economic and Security Review Commission.P 444
- <sup>54</sup> Kozy, A.. "U.S.- China Commission". Twitter Tweet. 2/17/2022
- <sup>55</sup> Aitel, D., et al, 2022.
- <sup>56</sup> Zhou, C., Gao, Y., Fu, A., Chen, K., Zhang, z., Xue, M., Zhang, Y.. "PPA: Preference Profiling Attack Against Federated Learning". School of Computer Science and Engineering, Nanjing University of Science and Technology, China. Paper. 10/29/2022. P 1
- <sup>57</sup> China Defense Universities Tracker. Database query "Cyber," Australian Strategic Policy Institute.
- <sup>58</sup> Alston, Bird. "DOJ Indicts Chinese Military Personnel for Involvement in 2017 Equifax Breach". Web article. JDSupra. URL: <https://www.jdsupra.com/legalnews/doj-indicts-chinese-military-personnel-60076>. 2/12/2020. Accessed: 5/25/2023
- <sup>59</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 30. Citing: China Defense Universities Tracker, "Shanghai Jiao Tong University," Australian Strategic Policy Institute, November 18, 2019; China Defense Universities Tracker, "Southeast University," Australian Strategic Policy Institute, November 12, 2019
- <sup>60</sup> Cary, D.. 2/17/2022. P 4
- <sup>61</sup> Doshi, B., Bello-Ogunu, E., Clouse, D., Cardinal Stakenas, A., craven, R., Jenks, J., Kimball, R., Kott, A., Lovend, M., Mathews, J., Robb, P.. "Technology trends and Impact on Cyber Battleground". Cyber CoI. Study. 1/20/2022. P 8, Quoting from the National Security Council AI Strategy.

---

<sup>62</sup> Doshi, B., Bello-Ogunu, E., Clouse, D., Cardinal Stakenas, A., craven, R., Jenks, J., Kimball, R., Kott, A., Lovend, M., Mathews, J., Robb, P.. "Technology trends and Impact on Cyber Battleground". Cyber Col. Study. 1/20/2022. P 8

<sup>63</sup> Barnes, J.. "How the Computer Chip Shortage Could Incite a U.S. Conflict With China". New York Times Online. Web Article. 1/26/2022.

<sup>64</sup> Che, C., Liu, J.. "'De-Americanize': How China Is Remaking Its Chip Business". New York Times Online. Web Article. 5/11/2023. P

<sup>65</sup> "Rare-earth element". Wikipedia. Encyclopedia Article. URL: [https://en.wikipedia.org/wiki/Rare-earth\\_element](https://en.wikipedia.org/wiki/Rare-earth_element). Accessed: 5/25/2023

<sup>66</sup> Baruzzi, S.. "China's Export Control Law Explained". China Briefing. Article. 11/9/2020.

<sup>67</sup> "2023 Global Threat Report". Crowdstrike. Report. P 28

<sup>68</sup> Bowman, J.. "A Modern Great Wall: PRC Smart Cities and the A2/AD Implications for AFSOC". Naval Postgraduate School. Thesis. 6/2022.

<sup>69</sup> Bowman, J. P 39

<sup>70</sup> Laudun, J, et al. "The Department of Defense's Multidomain Operations Challenge". Global Security Review. Article. 6/16/2022. P 6.

<sup>71</sup> Doshi, B., et al.

<sup>72</sup> Stefanick, T.. "The State of U.S.- China Quantum Data Security Competition". Brookings Institute. Article. 9/18/2020. P 7

<sup>73</sup> Stefanick, T. P 7

<sup>74</sup> Doshi, B., et al. P 39

<sup>75</sup> Stefanik, T. P 7

<sup>76</sup> "Chinese Intelligence Repurposed NSA Tools to Attack Private Companies". Council on Foreign Relations. Report. 5/2019.

<sup>77</sup> "Understanding Government Timelines to Award". MITRE Corp. Web Page. URL: <https://aida.mitre.org/demystifying-dod/timelines/>. Accessed: 5/2/2023.

<sup>78</sup> "DOD Should Develop a Strategy for Assessing Contract Award Time Frames". GAO. Report. 7/2018

---

<sup>79</sup> Naughter, T.. "The Importance of a Post-Award Kick-Off Meeting in Contract". Contractworks. Web Page. URL: <https://www.contractworks.com/blog/the-importance-of-a-post-award-kick-off-meeting-in-contract-management>. 12/14/2017. Accessed: 5/2/2023

<sup>80</sup> Joyce, K.. "DoD Cybersecurity Requirements: Tips for Compliance". Netwrix. Blog. URL: [https://blog.netwrix.com/2022/09/28/dod\\_cyber\\_security\\_requirements/](https://blog.netwrix.com/2022/09/28/dod_cyber_security_requirements/). 3/17/2023. Accessed: 5/2/2023

<sup>81</sup> Handler, Simon. "The 5x5 - China's cyber operations". Discussion with John Costello. Atlantic Council. 1/30/2023. P 2.

<sup>82</sup> Lau, L.. "Inside the Persistent Mind of a Chinese Nation-State Actor". Secureworks. Presentation. 1/27/2022. Slide 8.

<sup>83</sup> "China's National Defense in a New Era". Government of the PRC. 7/24/2019, as reported in Wikipedia article "People's Liberation Army Strategic Support Force". URL: [https://en.wikipedia.org/wiki/People's\\_Liberation\\_Army\\_Strategic\\_Support\\_Force](https://en.wikipedia.org/wiki/People's_Liberation_Army_Strategic_Support_Force). Accessed 4/3/2023

<sup>84</sup> Cimpanu, C.. "China has been 'Hijacking the vital internet backbone of western countries'". ZDNet. Web article. 10/31/2018. URL: <https://www.zdnet.com/article/china-has-been-hijacking-the-vital-internet-backbone-of-western-countries/>. Accessed: 3/22/2023.

<sup>85</sup> Chakravarti, J.. "Google Suspends Chinese App Following Malware Discovery". Information Security Media Group. Article. 3/21/2023.

<sup>86</sup> Jili, Bulelani. P6.

<sup>87</sup> "The Chinese Private Sector Cyber Landscape".. Margin Research. Paper. 4/25/2023. P 2

<sup>88</sup> "2022 Global Threat Report". CrowdStrike. Report. 9/28/2022. P 17

<sup>89</sup> "2023 Global Threat Report". CrowdStrike. Report. P 28

<sup>90</sup> "Chinese State-Sponsored Group TA413 Adopts New Capabilities in Pursuit of Tibetan Targets". Recorded Future. Insikt Group. Report. 9/22/2022.

<sup>91</sup> Work, J.D. P 5

<sup>92</sup> Patel, T.. "Signature Management using Operational Knowledge and Environments (SMOKE)". DARPA. Proposer's Brief. 12/7/2021. P 4

<sup>93</sup> Meadors, T., LTCdr. "Five Cyber Metrics Every Naval Officer Needs to Know". U.S. Naval Institute -Proceedings, Vol. 149/6/1,444. Article. 6/2023.

- 
- <sup>94</sup> Uren, T., Hogeveene, B. and Hanson, F. "Defining Offensive cyber capabilities". Report. Australian Strategic Policy Institute. URL: <https://www.aspi.org.au/report/defining-offensive-cyber-capabilities>. 74/2018. Accessed: 3/28/2023. P 1.
- <sup>95</sup> Uppal, R.. "DARPA EA Developed Tools for Timely, Accurate Threat Information and Attribution of Malicious Cyber Actors like Russia and China.". International Defense, Security & Technology (CA, USA). Quoting Michael Angelo. Article. 3/10/2022. P 3
- <sup>96</sup> "10 Chinese Weapons That Were Copied From USA". The Buzz YouTube Channel. Video. URL: [https://www.youtube.com/watch?v=CRLJID\\_bbuA&list=RDLVCRLJID\\_bbuA&start\\_radio=1&rv=CRLJID\\_bbuA&t=0](https://www.youtube.com/watch?v=CRLJID_bbuA&list=RDLVCRLJID_bbuA&start_radio=1&rv=CRLJID_bbuA&t=0) Posted: 9/23/2021. Accessed: 5/30/2023.
- <sup>97</sup> Huang, Y.. "China's Record on Intellectual Property Rights Is Getting Better and Better". Foreign Policy. Web Page. URL: <https://foreignpolicy.com/2019/10/16/china-intellectual-property-theft-progress/>. 10/16/2019. Accessed 3/28/2023
- <sup>98</sup> "China Says U.S. Hacked University With 'Drinking Tea' Cyber-Sniffing Weapon". Newsweek. Web Article. 9/26/2022
- <sup>99</sup> Raud, M., P 9
- <sup>100</sup> Singh, M.. "China's Cyber Warfare Capabilities". Indian Defence Review. Article. 7/11/2020. URL: <http://www.indiandefencereview.com/news/chinas-cyber-warfare-capabilities/>. Accessed: 5/5/2023
- <sup>101</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 15
- <sup>102</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 17
- <sup>103</sup> Dille, G.. "FBI, DHS: China Postes Biggest Long-Term Cyber Threat to US". Meritalk. Article. 11/18/2022. P 1
- <sup>104</sup> Starks, T.. "China getting bolder and better in cyberspace, spy chief warns". Washington Post. Article. 3/9/2023. P 2, 3
- <sup>105</sup> "Advanced Persistent Threats (APTs)". Mandiant. Web-based Report. 2023.
- <sup>106</sup> "APT1 Exposing One of China's Cyber Espionage Units". Mandiant. Report. 9/13/2021. P 3
- <sup>107</sup> Handler, Simon. P 2.
- <sup>108</sup> Martin, A.. "Chinese Security Researchers Claim to Have Identified 'Against the West' Hackers". Recorded Future. Article. 2/20/2023

---

<sup>109</sup> Handler, Simon. P 5.

<sup>110</sup> Handler, Simon. P 2.

<sup>111</sup> Davidpur, Niv. "Which Countries are Most Dangerous? Cyber Attack Origin – by Country". Webpage. CyberProof.com. URL: <https://blog.cyberproof.com/blog/which-countries-are-most-dangerous>. 1/4/2022. Accessed 3/24/2023.

<sup>112</sup> Sucio, Peter. "The Not-So Secret Cyber War: 5 Nations Conducting the Most Cyberattacks". Article. ClearanceJobs. URL: <https://news.clearancejobs.com/2022/10/17/the-not-so-secret-cyber-war-5-nations-conducting-the-most-cyberattacks/>. 10/17/2022. Accessed: 3/24/2023

<sup>113</sup> Plis, Michael. "Top 10 countries where security hackers come from & their types". Webpage. Cyberkite. URL: <https://www.cyberkite.com.au/post/hackers-top-10-countries-where-they-come-from-hacker-types#viewer-9hced>. 7/22/2023. Accessed: 3/24/2023

<sup>114</sup> Sharwood, Simon. "FBI says more cyber attacks come from China than everywhere else combined". Article. The Register. URL: [https://www.theregister.com/2022/02/03/fbi\\_china\\_threat\\_to\\_usa/](https://www.theregister.com/2022/02/03/fbi_china_threat_to_usa/). 2/3/2022. Accessed: 3/24/2023

<sup>115</sup> "2023 Global Threat Report- Executive Summary". CrowdStrike. Report. P 5

<sup>116</sup> Hodgson, Q., Shokh, Y., Balk, J. " Many Hands in the Cookie Jar. Rand Corp. Case Studies Report. RR=A1190-1. 4/20/2022. P 14

<sup>117</sup> Gompert, D. and Binnendijk, H.. "The Power to Coerce: Countering Adversaries Without Going to War". RAND Corp. Report RR-1000-A. 2016, p. 35. as referenced by Heath, T.. " U.S. Strategic Competition with China." Rand Corp.. Research Primer. 6/2021. P 11-12

<sup>118</sup> "CYBER 101 - Defend Forward and Persistent Engagement". U.S. Cyber Command-News. Article. 10/25/2022.

<sup>119</sup> Poindexter, Z.. "Effects of Defend Forward on Security, Stability and U.S. Interests in the Cyberspace Domain". Naval Postgraduate School. Thesis. 6/2022. P v

<sup>120</sup> Denning, D.. "How the Chinese Cyberthreat Has Evolved". Scientific American. Article.10/7/2017. P 1. Reprinted from the online publication "The Conversation".

<sup>121</sup> Liptak, K.. "US blames China for hacks, opening new front in cyber offensive". CNN. Article. URL: <https://www.cnn.com/2021/07/19/politics/us-china-cyber-offensive/index.html>. 7/19/2021. Accessed 4/12/2023

---

<sup>122</sup> Erica D. Borghar and Shawn W. Lonergan. "Chinese Hackers are Stealing U.S. Defense Secrets: Here is How to Stop Them". Net Politics, Council on Foreign Relations. 3/11/2019. P 3-4.

<sup>123</sup> Singh, M.

<sup>124</sup> Tanner 2017, p. 92; Faith Hung, "Taiwan Stock Selloff Seen Continuing as New President Takes Power," Reuters, January 22, 2016. as referenced in: Lin, B., Garafola, C., McClintock, B., Blank, Hornung, J., Schwindt, J., Moroney, J., Orner, P., Borrmann, D., Denton, S., Chambers, J.. " Competition in the Gray Zone- Countering China's Coercion Against Allies and Partners in the Indo-Pacific". Rand Corp.. Research report. RR-A594-1. 2022. P 59

<sup>125</sup> " Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information Including Infectious Disease Research". United States Department of Justice News. Press Release. 7/19/2021. P 2

<sup>126</sup> "Potential for China Cyber Response to Heighten U.S.-China Tensions". NSA, CISA & FBI. Cybersecurity Advisory. 10/20/2020

<sup>127</sup> "2023 Global Threat Report- Executive Summary". CrowdStrike. Report. P 5

<sup>128</sup> "The NSA Hacked Huawei Long Ago". Cyber Security Intelligence. Web Article. 9/15/2022.

<sup>129</sup> Kagubare, I.. "Cyberspace plays key role in growing US-China tension". The Hill. Article. 6/6/2023.

<sup>130</sup> Stockton, P.. "Defeating Coercive Information Operations in Future Crises". Johns Hopkins, APL. Report. 2021. P 44

<sup>131</sup> 2022 Annual Threat Assessment of the U.A. Intelligence Community. Director of National Intelligence Report. 3/6/2022. P 8.

<sup>132</sup> Mesich, M.. " China Is Targeting America's Critical Infrastructure. Here's What You Can Do About It.". Industrial Defender. Article. URL: <https://www.industrialdefender.com/blog/china-targeting-american-critical-infrastructure>. 6/29/2022. Accessed: 3/28/2023. P 1.

<sup>133</sup> "2023 Global Threat Report". CrowdStrike. Report. P 25

<sup>134</sup> Jili, Bulelani. P 6.

<sup>135</sup> "CYBER 101 - Defend Forward and Persistent Engagement". U.S. Cyber Command. Article. 10/25/2022. URL: <https://www.cybercom.mil/Media/News/Article/3198878/cyber-101-defend-forward-and-persistent-engagement/>. Accessed: 4/12/2023. P 1

---

<sup>136</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 18

<sup>137</sup> "2022 Report to Congress". U.S. China Economic and Security Review Commission. Report. 11/2022. P 418

<sup>138</sup> Mazarr, M., Frederick, B., Ellinger, E., Boudreaux, B.. "Competition and Restraint in Cyberspace". RAND. Report. 2022. P xii

<sup>139</sup> Mazarr, M., et al. P 8

<sup>140</sup> Handler, Simon. P 5.

<sup>141</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 1

<sup>142</sup> Handler, Simon. P 5.

<sup>143</sup> 2019 National Defense Authorization Act. 105th U.S. Congress.

<sup>144</sup> "Strategic Cyberspace Operations Guide". Amy War College. Handbook. 9/28/2022. P 15

<sup>145</sup> Siraj, N.. "NSA's Cyberattacks on China Expose New Face of U.S. Imperialism". cgtn.com. Web Article. 9/13/2022.

<sup>146</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 1

<sup>147</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 28

<sup>148</sup> "The Chinese Private Sector Cyber Landscape".. Margin Research. Paper. 4/25/2023. P 2

<sup>149</sup> MacGhillionn, J. P 3.

<sup>150</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 30. Citing: China Defense Universities Tracker, "Shanghai Jiao Tong University," Australian Strategic Policy Institute, November 18, 2019; China Defense Universities Tracker, "Southeast University," Australian Strategic Policy Institute, November 12, 2019

<sup>151</sup> Harold, S., Libick, M., Cevallos, A.. P viii

<sup>152</sup> China Cyber Expert Dakota Cary suggests that China might be exploiting agreements or compromises of telecommunication giants in order to collect directly from the internet backbone or undersea cables. These covert access points would afford them operational advantages.



- <sup>153</sup> Poindexter, Z.. P 34
- <sup>154</sup> "A New Framework for Understanding and Countering China's Gray Zone Tactics". Rand Corp.. Research Brief. RB-A594-1. 2022. P 1, 3
- <sup>155</sup> "A New Framework for Understanding and Countering China's Gray Zone Tactics". P 5
- <sup>156</sup> Stockton, P. P 9
- <sup>157</sup> Martin, B., Gunness, K., DeLuca, P., Shostak, M.. "Implications of a Coercive Quarantine of Taiwan by the Peoples Republic of China". Rand Corp. Research Report. RR-A1279-1. 2022. P 11-12
- <sup>158</sup> Harold, S., Beauchamp-Mustafaga, N., Hornung, J.. "Chinese Disinformation Efforts on Social Media". RAND. Report. 2021. P 2
- <sup>159</sup> Fitri, A.. "What is the NSA Actually Doing in China". Tech Monitor. Article. 3/3/2023
- <sup>160</sup> "2022 Report to Congress". U.S. China Economic and Security Review Commission. Report. 11/2022. P 450
- <sup>161</sup> "2022 Report to Congress". U.S. China Economic and Security Review Commission. Report. 11/2022. P 443
- <sup>162</sup> Cheng, D. "China's Quest for Information Dominance". Association of Old Crows. Podcast "From the Crows Nest". 4/26/2023.
- <sup>163</sup> "TikTok promotes engineering and maths in China, while making youth in other countries addicted to twerking and porn". OpIndia. Article. URL: <https://www.opindia.com/2022/07/tiktok-china-engineering-other-countries-porn-twerking/>. 7/25/2022. Accessed 3/28/2030.
- <sup>164</sup> Lin, B., Garafola, C., McClintock, B., Blank, Hornung, J., Schwindt, J., Moroney, J., Orner, P., Borrmann, D., Denton, S., Chambers, J.. "Competition in the Gray Zone- Countering China's Coercion Against Allies and Partners in the Indo-Pacific". Rand Corp.. Research report. RR-A594-1. 2022. P 15
- <sup>165</sup> Handler, Simon. P 4.
- <sup>166</sup> "2023 Global Threat Report- Executive Summary". CrowdStrike. Report. P 5
- <sup>167</sup> O'Neill, P.. "How China Built a One-of-a-Kind Cyber-Espionage Behemoth to Last". MIT Technology Review. Article. 2/28/2022. P 2

- 
- <sup>168</sup> Moody, G.. "China Actively Collecting Zero-Days for use by it's Intelligence Agencies- Just like the West". TechDirt. Blog. 9/24/2018
- <sup>169</sup> Cushing, T." Did the NSA Continue to Stay Silent on Zero-Day Vulnerabilities Even after Discovering it had been Hacked?". TechDirt. Blog. 8/19/2016
- <sup>170</sup> Dembroski, M., Fitzpatrick, J. Rydzynski, P.. "China's Cyber Attacks: The current threat landscape". IronNet, Paper. 9/7/2021. P 12
- <sup>171</sup> Cipanu, C.. "Chinese hacking group APT31 uses mesh of home routers to disguise attacks". The Record. Web Article. URL: <https://therecord.media/chinese-hacking-group-apt31-uses-mesh-of-home-routers-to-disguise-attacks>. 7/20/2022. Accessed: 6/9/2023
- <sup>172</sup> Handler, Simon. P 1
- <sup>173</sup> O'Neill, P. P 2
- <sup>174</sup> Doyle, P.. " Rob Joyce: China represents biggest long-term cyberthreat". TechTarget. Article. 6/9/2022. P 2
- <sup>175</sup> "NSA, CISA and FBI Expose PRC State-Sponsored Exploitation of Network Providers, Devices". NSA News. Article. 6/8/2022/
- <sup>176</sup> Lakshmanan, R.. "China Accuses NSA's TAO Unit of Hacking its Military Research University". The hacker News. Web Article. 9/12/2022.
- <sup>177</sup> Aitel, D., et al. P 5
- <sup>178</sup> Arghire, I.. "Chinese Cyberspies Delivered Malware via Legitimate Software Updates". SecurityWeek. Article. 4/27/2023. P 3, 5
- <sup>179</sup> Lakshmanan, R.. "China Accuses NSA's TAO Unit of Hacking its Military Research University". The hacker News. Web Article. 9/12/2022.
- <sup>180</sup> Harold, et al. P 8
- <sup>181</sup> "Cyberattacks worldwide 2022". KonBriefing.com. Web page Dataset. Accessed: 5/18/2023.
- <sup>182</sup> Voo, J., et al.. "Cyber Capabilities and National Power: A Net Assessment". International Institute for Strategic Studies. Report. 6/28/2021. P 3; and "National Cyber Power Index 2020," Harvard University Belfer Center. 9/2020. P 38
- <sup>183</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 20

- 
- <sup>184</sup> "2022 Report to Congress". U.S. China Economic and Security Review Commission. Report. 11/2022. P 438
- <sup>185</sup> "APT1 Exposing One of China's Cyber Espionage Units". Mandiant. Report. 9/13/2021. P 3
- <sup>186</sup> "APT1 Exposing One of China's Cyber Espionage Units". Mandiant. Report. 9/13/2021. P 3
- <sup>187</sup> Hodgson, Q., Shokh, Y., Balk, J. " Many Hands in the Cookie Jar. Rand Corp. Case Studies Report. RR-A1190-1. 4/20/2022. P 27
- <sup>188</sup> "The Chinese Private Sector Cyber Landscape".. Margin Research. Paper. 4/25/2023. P 1
- <sup>189</sup> O'Neill, P. P 2
- <sup>190</sup> "The Chinese Private Sector Cyber Landscape".. Margin Research. Paper. 4/25/2023. P 2
- <sup>191</sup> Aitel, D., et al.
- <sup>192</sup> Lau, L.."Inside the Persistent Mind of a Chinese Nation-State Actor". Secureworks. Presentation. 1/27/2022. Slide 33.
- <sup>193</sup> Starks, T.."China getting bolder and better in cyberspace, spy chief warns". Washington Post. Article. 3/9/2023. P 2
- <sup>194</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 4
- <sup>195</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 19. Citing: International Institute for Strategic Studies, "Cyber Capabilities and National Power: A Net Assessment," June 28, 2021, 174; Helen Warrel, "China's Cyber Power at Least a Decade behind the US, New Study Finds," Financial Times, June 27, 2021.
- <sup>196</sup> Lakshmanan, R.. "China Accuses NSA's TAO Unit of Hacking its Military Research University". The hacker News. Web Article. 9/12/2022.
- <sup>197</sup> Laudun, J, Kroh, T, Siddiki, M., Arp, R. and Lowther, A.. "The Department of Defense's Multidomain Operations Challenge". Global Security Review. Article. 6/16/2022. P 5, 7, 12
- <sup>198</sup> "Cyberattacks in 2022". KonBriefing. Web page. URL: <https://konbriefing.com/en-topics/cyber-attacks-2022.html>. Accessed: 03/29/2023
- <sup>199</sup> "NCC Group Annual Threat Monitor 2022". NCC Group. Report. 2/8/2023. P 46
- <sup>200</sup> "Federal Cybersecurity: America's Data Still at Risk". U.S. Senate Committee on Homeland Security and Governmental Affairs. Staff Report. 8/2021. P ii

---

<sup>201</sup> "Potential for China Cyber Response to Heighten U.S.- China Tensions". NSA, CISA & FBI. Cybersecurity Advisory. 10/20/2020

<sup>202</sup> Barnes, J., Haberman, M., Swan, J.. "Chinese Hackers Breached Government Email Accounts, Microsoft Says". New York Times Online. Online Periodical. 7/12/2023.

<sup>203</sup> "Share of the population using the internet in the past 3 months". Our World in Data. Interactive online chart. URL: <https://ourworldindata.org/grapher/share-of-individuals-using-the-internet?country=CHN~USA>. Accessed: 4/14/2023

<sup>204</sup> McCarthy, N.. "China Now Boasts More Than 800 Million Internet Users and 98% Of Them Are Mobile". Forbes.com. Infographic. URL: <https://www.forbes.com/sites/niallmccarthy/2018/08/23/china-now-boasts-more-than-800-million-internet-users-and-98-of-them-are-mobile-infographic/?sh=52f502a37092>. 8/23/2018.. Accessed: 4/14/2023

<sup>205</sup> "Internet in China". Wikipedia. Website. URL: [https://en.wikipedia.org/wiki/Internet\\_in\\_China](https://en.wikipedia.org/wiki/Internet_in_China). Accessed: 4/14/2023

<sup>206</sup> SOURCE: U.S. Census Bureau, Current Population Survey, Annual Social and Economic Supplement, 2018.

<sup>207</sup> "Desktop/laptop ownership among adults in the United States from 2008 to 2019". Statista.com. Infographic. URL: <https://www.statista.com/statistics/756054/united-states-adults-desktop-laptop-ownership/>. Accessed: 4/14/2023

<sup>208</sup> Slotta, D. "Number of computers per 100 households in China 2000-2021". Statista. Webpage. URL: <https://www.statista.com/statistics/278758/number-of-computers-per-100-households-in-china/>. Accessed 4/14/2023

<sup>209</sup> Gopal, D., McMullen, L., Walls, A., Addiscott, R., Furtado, P., Porter, C., Isaka, O., Winckless, C.. "Gartner Predicts 2023 Cybersecurity Industry Focuses on the Human Deal". Gartner Group. Website version. 1/25/2023. Referencing "Data Breach Investigation Report" by Verizon, Corp.

<sup>210</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 43

<sup>211</sup> "2023 Global Threat Report" CrowdStrike. Report. P 2.

<sup>212</sup> Uppal, R.. "DARPA EA Developed Tools for Timely, Accurate Threat Information and Attribution of Malicious Cyber Actors like Russia and China.". International Defense, Security & Technology (CA, USA). Article. 3/10/2022. P 2

- 
- <sup>213</sup> "People's Republic of China State- Sponsored Cyber Actors Exploit Network Providers and Devices". CISA. Website. 6/10/2022. URL: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-158a>. Accessed: 4/4/2023. P 4.
- <sup>214</sup> Uppal, R.. "DARPA EA Developed Tools for Timely, Accurate Threat Information and Attribution of Malicious Cyber Actors like Russia and China.". P 3
- <sup>215</sup> "2023 Global Threat Report" Crowdstrike. Report. P 2.
- <sup>216</sup> O'Neill, P. P 2
- <sup>217</sup> "The NTT security holdings 2022 global threat intelligence report a year of more sophisticated and substantial threats". Cyber Threat Alliance. Webinar. URL: <https://www.cyberthreatalliance.org/cta-webinar-the-ntt-security-holdings-2022-global-threat-intelligence-report-a-year-of-more-sophisticated-and-substantial-threats-2/>. Accessed: 3/13/2023
- <sup>218</sup> Uppal, R.. "Nation Backed Cyber Attacks Led by Russia, China, North Korea and Iran for Cyber Espionage and Intellectual Property Theft". International Defense Security & Technology. Article. 3/16/2023. P 5
- <sup>219</sup> "TikTok is Banned from British Government Phones". Cybersecurity Intelligence. Web Article. 3/17/2023
- <sup>220</sup> "The Chinese Private Sector Cyber Landscape".. Margin Research. Paper. 4/25/2023. P 4. Quote from Zheng Wenbin.
- <sup>221</sup> Roberts, P.. "Gaps in the NVD Increasing U.S. Cyber Threat". ReversingLabs. Blog. 9/26/2022. P 4
- <sup>222</sup> Moriuchi, P., Ladd, B.. "China's Ministry of State Security Likely Influences National Network Vulnerability Publications". Insikt Group. Recorded Future Blog. 11/16/2017. Accessed: 7/13/2023
- <sup>223</sup> Roberts, P. P 5
- <sup>224</sup> Roberts, P. P 5
- <sup>225</sup> Moriuchi, P., Ladd, B.
- <sup>226</sup> Cronk, T. M.. "Hicks: Governance Differences Between U.S., China Are in Sharp focus". DoD News. Article. 3/19/2021. P 5
- <sup>227</sup> Seldin, J. "U.S., Albania on 'Hunt' for Iranian Cyber Actors". Voice of America News. Article. 3/23/2023. P 1.

- 
- <sup>228</sup> "DISA announces successful completion of Thunderdome prototype". DISA Office of Strategic Communications. Article. 3/6/2023. P 1.
- <sup>229</sup> Beitsch, R.. "DOJ scraps Trump-era China Initiative for broader national security program". The Hill. Article. URL: <https://thehill.com/policy/national-security/595549-doj-scraps-trump-era-china-initiative-for-broader-national-security>. 2/23/2022. Accessed: 4/26/2023
- <sup>230</sup> Vicens, A..” DOJ establishes cybercrime enforcement unit as U.S. warnings mount over Chinese hacking Cyberscoop. Web article. 6/20/2023. URL: <https://cyberscoop.com/doj-establishes-cybercrime-enforcement-unit-natseccyber/>. Accessed: 7/17/2023
- <sup>231</sup> "FY2024 Performance Budget Congressional Submission". US Department of Justice National Security Division. Congressional Budget Document. 3/8/2023. URL: [extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.justice.gov/d9/2023-03/nsd\\_fy\\_2024\\_pb\\_narrative\\_03.08.23\\_omb\\_cleared.pdf](https://www.justice.gov/d9/2023-03/nsd_fy_2024_pb_narrative_03.08.23_omb_cleared.pdf). Accessed:7/17/23. P51
- <sup>232</sup> Croft, D. " Diplomacy Won't Slow China's Cyber Attacks, Says Former NSA Head". MomentumMedia Cybersecurity Connect. Article. 3/6/2023
- <sup>233</sup> Perez, L. ."DIA Plans 'China Mission Group' to Monitor Threats". MeriTalk. Article. 11/30/2022. P 1.
- <sup>234</sup> "TikTok is Banned from British Government Phones". Cybersecurity Intelligence. Web Article. 3/17/2023
- <sup>235</sup> Lyons, K.. "China tells government offices to remove all foreign computer equipment". The Guardian. Article. URL: <https://www.theguardian.com/world/2019/dec/09/china-tells-government-offices-to-remove-all-foreign-computer-equipment>. 12/8/2019. Accessed: 4/27/2023. P 1
- <sup>236</sup> Poindexter, Z P 34
- <sup>237</sup> Che, C., Liu, J..
- <sup>238</sup> Keller, J.. "Packet Forensics pursues DARPA trusted computing project to devise cyber security for network botnet attacks. Military & Aerospace Electronics. Article. 9/5/2019
- <sup>239</sup> Keller, J.
- <sup>240</sup> Kline, Allison. "Harnessing Autonomy for Countering Cyberadversary Systems (HACCS). DARPA. Article. URL: <https://www.darpa.mil/program/harnessing-autonomy-for-countering-cyberadversary-systems>. Accessed: 4/4/2023
- <sup>241</sup> Metrick, K., Semrau, J., Sadayappan. S.. “Disclosure, Patch Release and Vulnerability Exploitation — Intelligence for Vulnerability Management, Part Two”. Mandiant. Report.

---

10/29/2021. URL: <https://www.mandiant.com/resources/blog/time-between-disclosure-patch-release-and-vulnerability-exploitation>. Accessed: 7/18/23. Figure 1

<sup>242</sup> Metrick, K., et al

<sup>243</sup> Metrick, K., et al. Figure 2

<sup>244</sup> "People's Republic of China State- Sponsored Cyber Actors Exploit Network Providers and Devices". CISA. Website. 6/10/2022. URL: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-158a>. Accessed: 4/4/2023. P 4.

<sup>245</sup> Metrick, K., et al. Figure 2

<sup>246</sup> "Threat Trends Breaking Down the 2022 M-Trends report ". The Defender's Advantage Podcast. Mandiant. Podcast. 2022.

<sup>247</sup> "2023 Global Threat Report". Crowdstrike. Report. P 9

<sup>248</sup> Narang, S. "Top 20 CVEs Exploited by People's Republic of China State-Sponsored Actors (AA22-279A)". Tenable Blog. Report. 10/7/2022.

<sup>249</sup> "2022 Global Threat Report". Crowdstrike. Report. 9/28/2022. P 3

<sup>250</sup> "Federal Cybersecurity: America's Data Still at Risk". U.S. Senate Committee on Homeland Security and Governmental Affairs. Staff Report. 8/2021. P ii

<sup>251</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 4

<sup>252</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 1

<sup>253</sup> " Chinese State-Sponsored Cyber Operations: Observed TTPs". National Security Agency, Cybersecurity & Infrastructure Security Agency and the Federal Bureau of Investigation. Cybersecurity Advisory. 7/19/2021. P 3

<sup>254</sup> "2022 Report to Congress". U.S. China Economic and Security Review Commission. Report. 11/2022. P 448

<sup>255</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 6. Quoting from: Xi Jinping, "Speech at the National Cybersecurity and Informationization Work Conference"

<sup>256</sup> "Federal Cybersecurity: America's Data Still at Risk". U.S. Senate Committee on Homeland Security and Governmental Affairs. Staff Report. 8/2021. P ii



<sup>257</sup> MacGhillionn, J.. P 4.

<sup>258</sup> Uppal, R.. "Nation Backed Cyber Attacks Led by Russia, China, North Korea and Iran for Cyber Espionage and Intellectual Property Theft". P 3

<sup>259</sup> "2023 Global Threat Report- Executive Summary". Crowdstrike. Report.

<sup>260</sup> Geller, E.. "Weekly Cybersecurity-Education- Do we have your attention?". Politico. Newsletter. 8/22/2022.

<sup>261</sup> "2023 Cybersecurity Almanac". Momentum Cyber. Report. 2/22/2023. P 14

<sup>262</sup> Jiang, T.. "From Offense Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar". Shanghai International Studies University, School of International Relations and Public Affairs. P. R. China. Paper. 8/2/2019. P 4

<sup>263</sup> Cary, D.. "Dakota Cary's Testimony Before the U.S.- China Economic and Security Commission". UCESRC. Testimony. 2/17/2022. P 5

<sup>264</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 3

<sup>265</sup> Cary, D.. "Dakota Cary's Testimony Before the U.S.- China Economic and Security Commission". UCESC. Testimony. 2/17/2022. P 3

<sup>266</sup> "A New Framework for Understanding and Countering China's Gray Zone Tactics". Rand Corp.. Research Brief. RB-A594-1. 2022. P 8

<sup>267</sup> Roberts, P. P 5

<sup>268</sup> Nissen, C., Clancy, C., Ledgett, R., Sledjeski, C. "Beyond Solarwinds: Principles for Securing Software Supply Chains". MITRE Corp. Report 21-0843. 3/18/2021. P 3, 7

<sup>269</sup> Handler, Simon. P 5.

<sup>270</sup> "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States". U.S.-China Economic and Security Review Commission. Book Chapter (2). 11/7/2022. P 1

<sup>271</sup> Erica D. Borghar and Shawn W. Lonergan. "Chinese Hackers are Stealing U.S. Defense Secrets: Here is How to Stop Them". Net Politics, Council on Foreign Relations. 3/11/2019. P 5.

<sup>272</sup> Borghar and Lonergan.. P 6.