What are the main differences between the economic and military dimensions of the United States' and China's cybersecurity policies?

Rajveer Mohit Batra
Dhirubhai Ambani International School, rajveerbatra11@gmail.com

Acknowledgements
Thank you to my mentor, Tomass Pildegovičs, from Cambridge University, for your guidance in the development of this research paper.

Abstract:

The world's two most powerful economies, China and the United States, rely on the global digital domain for economic productivity, societal well-being, and national security. At the same time, governments and companies alike are becoming increasingly concerned about the security and reliability of their information systems, even as there remains significant ambiguity about the true nature of the threats and the most effective ways of addressing them. In recent years, the security of global information networks has been a contentious issue in US-China relations. Against this backdrop, this paper seeks to appraise and analyze the variations in strategies and methods used by the United States and China to pursue their military and economic interests the cyber domain. This paper concludes by outlining the threat landscape that characterizes US-China relations in the cyberspace, as well as maps the way forward for bridging gaps in trust and strengthening international cooperation frameworks.

I. Introduction

Since the advent of a commercialized internet in the early 1990s, digital technology has become integrated in nearly every facet of economic and social life. It is difficult to overlook the consequences that technology and the internet have on today's society, whether it be advancements in the medical field, speedier modes of transportation and communication, or the means through which governments conduct international diplomatic negotiations. However, the growing number of people using the internet has coincided to the proliferation of risks and security vulnerabilities. As several high-profile cybersecurity breaches and hacks from around the world have shown, cybersecurity is not just a national issue, but rather a transnational one with increasing geopolitical implications.

The world's two most powerful economies, China and the United States, rely on the global digital domain for economic productivity, societal well-being, and national security. At the same time, governments and companies alike are becoming increasingly concerned about the security and reliability of their information systems, even as there remains significant ambiguity about the true nature of the threats and the most effective ways of addressing them. In recent years, the security of global information networks has been a contentious issue in US-China relations. Chinese intrusions of the electronic systems of private corporations and key government institutions have risen in recent years, stoking political tension and further undermining trust in international norms. At the same time, computer hosts in the United States are responsible for a large portion of the malicious activities across the world. The US Department of Defense and the Chinese People's Liberation Army (PLA) both see cyberspace as a new battlefield. Nationalist "hacktivism," manifested in website defacements, service denials, and network exploitation, has been employed reciprocally in both directions across the Pacific.[1] This adverse situation

[1] *IGCC, Lindsay, Jon, April 2012 China/Cybersecurity*, http://www.bdo3c.f-sc.org/archives/921.pdf.

exacerbates mistrust and raises suspicions about the intentions and activities of the other in both Washington and Beijing.

II. Context and Background

To gain a better understanding of the current state of affairs between the United States and China in the cyberspace, one must first consider how the global community is dealing with the exponential growth and proliferation of technology. In addition to the established operational domains of air, sea, land, and space, the international community is currently adapting to cyberspace effectively becoming the fifth realm of activity. In 2013, Edward Snowden disclosed classified information from the US National Security Agency (NSA), exposing the United States' international abuse of cyber instruments for mass surveillance and espionage[2]. As a consequence, fifteen countries, from around the world, agreed that international law should provide clear rules, norms, and definitions for the cyberspace. To date, approximately forty governments in the international community have developed military cyber capabilities.[3]

Against this backdrop, this paper is animated by the urgent need to appraise and analyze the variations in strategies and methods used by the United States and China to pursue their military and economic interests the cyber domain. Broadly conceived, the two actors, despite divergent political systems and societal normative structures, demonstrate similar patterns of behavior and willingness to use similar instruments to defend national security objectives in the cyber domain. The policy of the United States in this regard is to maintain peace in the cyber realm by the use of force. China has taken a similar approach, and has even developed new tactics and training for its armed personnel to prepare for cyber assaults or espionage.

In recent years, the relationship between China and the United States has grown increasingly competitive and strained along several axes of confrontation. As previously stated, the purported cyber-attacks launched by the United States and China against each other and other adversaries have gained newfound prominence on the global political agenda. It is also critical to consider their relationship not only through a military lens, but also take into account economic, societal and other strategic dimensions. Critics of the US-China relationship believe that the two countries have been pushing each other's boundaries for too long and that if de-escalatory mechanisms are not instated, their systemic rivalry may spill over into conflict. When it comes to cybersecurity, many of those who see the value of a solid partnership regarded the agreement (2015 U.S. - China Cybersecurity Agreement) between US and China as a beacon of hope. They regarded it as a framework with the potential to serve as a template for shaping a better future for the whole international community, not just the world powers. Unfortunately, the agreement did not survive much considering both parties performed acts that ranged from aggravating to unlawful against one other in the cyber space. Within two years of the signing of the 2015 US-China Cybersecurity Agreement, the issue of Chinese intellectual property theft had not abated, but rather took on a new shape. Within the PRC, hacking organizations began targeting their own populace. Instead of focusing on corporate intellectual property theft in the United States, they too instead focused on a type of governmental espionage.

Because of the extraordinary power that the United States and China wield in the international arena, the geopolitical implications of their conduct and relationship in cyberspace are enormous. To curb the proliferation and misuse of technology, the two superpowers have the means to pursue a path of cooperation, including a potential resuscitation of the 2015 U.S.-China Cybersecurity Agreement, as well as investing political capital to reinforcing the pledge to collective action. If partnership between the two superpowers becomes a reality, the entire international community will profit. If a sustainable equilibrium of co-existence in cyberspace is not attained, the destructive potential will be enormous, and no single party if likely to prevail.

[2] "Edward Snowden: Leaks That Exposed US Spy Programme". *BBC News*, 2021, https://www.bbc.com/news/world-us-canada-23123964.
[3] ibid

III. China

Cyberwarfare was first discussed in Chinese intellectual circles in the 1990s, when it was referred to as "information warfare." Impressed by how the US military benefited from the use of high-tech weapons in the Gulf War – and subsequent operations in Kosovo, Afghanistan, and Iraq – China realised that it could not adequately defend itself without adapting to the changing nature of war, which demanded the integration of high-tech weapons, primarily information technologies, into its arsenal.[4] The Chinese cybersecurity law, which was enacted on November 7, 2016, by the Standing Committee of the National People's Congress, compels network operators to keep data on servers located within China and permits Chinese authorities to perform spot-checks on company network activities. In effect, this law is placed at the top of the cybersecurity legislative pyramid.

The major objectives of national cyber capabilities, in line with China's Military Strategy, are "cyberspace situation awareness, cyber defense, support for the country's cyberspace efforts, and involvement in international cyber cooperation." These goals are framed in the policy as “preventing catastrophic cyber disasters, guaranteeing national network and information security, and preserving national security and social stability.”

Cybereconomy

China has committed enormous investment to executing its national cyber development, IT and Big Data Strategies as well as the action plan "Internet Plus." It supports e-commerce development, promotes digital economy and real economy integration and works to optimise resource allocation and increase the overall productivity factor, which drives innovation, changes the economic structure and growth model.[5]

The US has grown increasingly aware that for China, cybersecurity is a profoundly economic and political matter, even if it is optically framed as a solely technological issue. At the same time, Western audiences largely lack a detailed understanding of the principles and policies that regulate the behaviour of Chinese private and public actors in the digital domain. This lack of knowledge and the consequent inability to comprehend China's internal economy and politics have the destructive potential to lead to a serious misinterpretation of its international conduct and ambition. Given that the bulk of daily insecurity in cyberspace is commercial and civilian in scope and nature, it is vital and relevant to examine the societal dimension of cybersecurity.

With the growth of the Internet and the vastly rising number of "netizens," online business and entertainment have flourished in China. However, Chinese netizens are constantly subjected to a range of security risks and barriers targeting and restricting their real or virtual economic gains. Behind those internet threats lies a sophisticated underground criminal economy fuelled by a range of mass data harvesting and collection techniques. Because of the differences between the Chinese economy, regulations, and culture and those of Western countries, the underground economy of information security in China is distinctive in many ways.[6] However, the research community has not paid enough attention to these concerns.

An examination of the underground economy's structure reveals the most profitable value chains and execution strategies, as well as the stages and responsibilities of various players. There are four value chains in the overall economy: 1) Theft of real assets, such as money from stolen bank accounts or credit cards; 2) Theft of network virtual assets, such as virtual cash and equipment, from stolen online gaming accounts and selling them for real money; 3) Abuse of Internet resources and services: using stolen Internet resources, such as compromised hosts, hacked servers, and infected smart phones, to benefit from Internet services; 4) Black hat tactics, tools, and

[4] Jinghua, Lyu. "What Are China’S Cyber Capabilities And Intentions?". *Carnegie Endowment For International Peace*, 2021, https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.
[5] Roberts, Huw et al. "The Chinese Approach To Artificial Intelligence: An Analysis Of Policy, Ethics, And Regulation". AI & SOCIETY, vol 36, no. 1, 2020, pp. 59-77. Springer Science And Business Media LLC, doi:10.1007/s00146-020-00992-2. Accessed 10 Sept 2021.
[6] G, Suresh. "Https://Medwinpublishers.Com/NNOA/NNOA16000183.Pdf". *Nanomedicine & Nanotechnology Open Access*, vol 5, no. 2, 2020. *Medwin Publishers*, doi:10.23880/nnoa-16000183.

training: selling Trojan horses and attack tools to offer technical assistance for cybercriminals, as well as giving rookie guidance.[7]

Cyberwarfare

Cyber capabilities are included in China's military policy as an area where the People's Liberation Army (PLA) should invest in capability development and integrate in operations on a wide scale.[8] Robert Gates, the former US Secretary of Defense, has also stated that the expansion of China's cyber toolbox is increasingly concerning, further exacerbating the trend of more than a decade of cyberattacks originating from China.[9]

Cyber capabilities, according to Chinese military strategists, represent a significant asymmetric instrument in a deterrent strategy. According to various analysis, an "important subject in Chinese publications on computer-network operations (CNO) is the use of computer-network attack (CNA) as the spear-point of deterrence"[10]. CNA raises the cost of the enemy's actions to the point where they are too high to justify coercive action as such, which Chinese strategists believe is an integral component of deterrence.[11] This may, for example, translate into providing China with the capacity to prevent the US from supporting Taiwan in a hypothetical conflict.[12]

According to analysts, China may have the world's most extensive coercive cyber warfare capability, which critically underpins Beijing's aspiration to consolidate and reinforce its "global-power status."[13] These conclusions are based on credible and verifiable Chinese literature on the issue, which conceives of cyberwarfare as an integral asymmetric weapon for balancing overwhelming (primarily US) strength, particularly in the event of open confrontation, but also as an instrument of deterrence.[14]

A 2008 MI5 document titled "The Threat from Chinese Espionage" has suddenly emerged into the public sphere in the United Kingdom. "Any UK firm may be at danger if it has information that may benefit the Chinese," according to the limited report.[15] In addition, the study details how China's cyberwarfare effort targeted British military, energy, telecommunications, and industrial sectors, as well as public relations and international law firms, some of which represent key components of British critical infrastructure.[16]

China's cyber espionage is growing increasingly sophisticated and mature in its approach, according to the British Joint Intelligence Committee, which coordinates operations between the two intelligence services, MI5 and MI6. It was described how China might use this to cut down critical utilities such as power, food, and water.[17] This is far from the first time the British have accused China of conducting aggressive cyber operations.

---

[7] *IGCC, Lindsay, Jon, April 2012 China/Cybersecurity*, http://www.bdo3c.f-sc.org/archives/921.pdf.
[8] Chen Zhou, "A Review of China's Military Strategy," China Armed Forces 1:1: 19.
[9] Lin Cheng-yi, "China's 2008 Defence White Paper: The view from Taiwan," China Brief IX:3: 14.
[10] James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," 257
[11] Ibid.
[12] Timothy L. Thomas, "Nation-state Cyber Strategies: Examples from China and Russia," in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds.), Cyber- power and National Security (Dulles, VA: Potomac Books, Inc. and NDU Press, 2009), 468; James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," 258.
[13] Stratfor, "China: Pushing Ahead of the Cyberwarfare Pack," September 2, 2021, avail- able at: http://tinyurl.com/5u6j4qc (www.stratfor.com/memberships/132785/analysis/20090225_china_pushing_ahead_cyberwarfare_pack).
[14] Qiao Liang and Wang Xiangsui, Unrestricted Warfare, Beijing: PLA Literature and Arts Publishing House, 1999, 29, 47, 211–212.
[15] David Leppard, "China bugs and burgles Britain," Times Online, available at: http://www.timesonline.co.uk/tol/news/uk/crime/article7009749.ece.
[16] ibid
[17] John F. Burns, "Britain Warned Businesses of Threat of Chinese Spying," New York Times, available at: http://www.nytimes.com/2010/02/01/world/europe/01spy.html.

In December 2007, the chief of MI5, the UK's domestic intelligence service, claimed that the country was under (cyber) attack by "Chinese state entities."[18]

When a state displays its cybersecurity capabilities to the world, it has a genuine deterrent impact. This occurred when the United States learned in 2009 that its electrical network had been hacked and that portions of the network could be turned off whenever the hacker desired.[19] Other reports, while doubtful of the scale of such breaches, claim that while the foreign invaders did not cause immediate harm, they left behind software bugs that could be used to impair this crucial infrastructure in the future.[20] This operation was attributed to China, and at the time, the US chief of counterintelligence claimed, "we have witnessed Chinese network activity within several of our electrical systems."[21] The fact that Americans were unable to safeguard their power grid is one crucial signal, suggesting more broadly that the US may face major difficulties in addressing the challenge posed by China's aggressive cyber program.[22] A notable catalyst in raising the relevance of cybersecurity among Western governments was the 2007 Russian-waged cyberwarfare campaign against Estonia following Tallinn's decision to remove a controversial Soviet World War II memorial. These attacks, which originated in Russia, temporarily disabled key government and bank websites and defaced numerous public internet pages. Pentagon cyber security specialist Sami Saydjari told the US Congress that "a similar mass cyberattack could leave the United States without power for six months – enough time for China to occupy Taiwan, or for Russia to occupy the United States."[23] Such statements, even if intentionally hyperbolic, highlight the vulnerability of critical infrastructure in the United States. At the moment, the United States is lagging behind China in terms of engineering training for cyber-related activities[24]

Another dimension of China's coercive military behaviour in cyberspace concerns intellectual property theft with grave national security implications. For instance, large volumes of data were copied during a forced electronic entry into the Joint Strike Fighter program in 2009.[25] According to US intelligence, the attack was traced back to China, later manifesting in mimicked designs in China's own fighter aircraft models. As further outlined by the American counterintelligence director stated that "our networks are being mapped," referring to American aviation traffic control, and warned of a situation in which "a fighter pilot can't trust his radar."[26]

In early 2015, the reputable German magazine Der Spiegel released a collection of documents given by Edward Snowden, a former NSA contractor. Snowden was a computer intelligence expert who released highly sensitive and secret material about the NSA to the Washington Post and the Guardian, among other media outlets. These papers proved what many had believed for a long time: that the similarities between China's sophisticated J-31 stealth fighter and the United States' F-35 were not accidental. Experts in the aviation sector have long claimed that the F-35 had a serious influence on the J-31. Snowden's revelations were the first evidence that the Chinese gained access to top secret F-35 data as a consequence of a data breach at a Lockheed Martin subcontractor.

---

[18] No author, "Spy Chief in Britain accuses China of cyber crime," New York Times, available at: http://tinyurl.com/68l8arm (www.nytimes.com/ 2007/12/02/world/europe/02iht-cyber.1.8557238.html).
[19] Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," Wall Street Jour- nal, available at: http://online.wsj.com/article/SB123914805204099085.html.
[20] "Cyber spies assault US power grid," Jane's Intelligence Digest. Simon Tisdall, "Cyber-warfare 'is growing threat,'" Guardian, available at: http://tinyurl.com/ylav6sg (www.guardian.co.uk/technology/2010/feb/03/ cyber-warfare-growing-threat); and Kate Connolly, "Germany accuses China of industrial espionage," Guardian, available at: http://tinyurl.com/n7ggep (www.guardian.co.uk/world/2009/jul/22/ger- many-china-industrial-espionage).
[21] "U.S. Steps Up Effort on Digital Defenses," New York Times.
[22] "Total gridlock—Cyber threat to critical infrastructure," Jane's Intelligence Review
[23] "Total gridlock—Cyber threat to critical infrastructure," Jane's Intelligence Review
[24] "Cyber spies assault US power grid," Jane's Intelligence Digest.
[25] U.S.-China Economic and Security Review Commission (USCC), 2009 Report to Congress of the U.S.-China Economic and Security Review Commission, 167; "U.S.: Cyberspies Attack Joint Strike Fighter Project—Report," Stratfor, available at: http://tinyurl.com/655lbou (www.stratfor.com/memberships/136342/sitrep/20090421uscyberspiesattackjointstrikefighterprojectreport)
[26] "Computer Spies Breach Fighter-Jet Project," Wall Street Journal

China's espionage operations, according to The Diplomat, were aimed at obtaining the radar designs, as well as specific engine schematics, among many other things.

IV. United States of America

Cybereconomy

As evidenced by key political and doctrinal documents, such as the final report of the president's 60-day cybersecurity review and the 2010 quadrennial intelligence evaluation of terrorist threats confronting the United States, US government authorities also recognise cybersecurity to be an essential priority area. At the same time, this growing awareness has not always translated into urgency and investment, as officials and public servants have often lacked the necessary training or expertise to engage with this issue in a comprehensive, whole-of-government approach. This was evident in President Barack Obama's May 29, 2009, East Wing press statement on cybersecurity, in which he listed the following threats as "digital infrastructure" threats: "cyber thieves trolling for sensitive information," "the disgruntled employee on the inside," "the lone hacker a thousand miles away," "organised crime," "the industrial spy," and "foreign intelligence services."[27] There is scant information on the presence or impact of these risks, which, when paired with such wide and ambiguous criteria, makes it very challenging to operationalise in terms of designing a relevant policy response or assessing its effectiveness. In the US, the ever-growing scope and magnitude of computer and server infrastructure presents a growing number of potential entry-points for malicious actors and other vulnerabilities to cyber-attacks. Over the last decade, there has been an increasing dependence on the web even on vital systems, from secure private networks (or from no networks at all) to critical infrastructure control systems.

Cyberwarfare

The United States, as a large industrialised economy, is heavily reliant on the Internet and, hence, has become increasingly vulnerable to cyberattacks by malign state and non-state actors alike. At the same time, owing to comparably sophisticated technology and a vast military budget, the United States possesses significant capabilities in both defence and power projection. Physical systems and infrastructures connected to the internet are becoming vulnerable to cyber warfare. However, the US has developed considerable cyber capabilities in response to these rising concerns.

The US Department of Defense sees the use of computers and the Internet to conduct cyberwarfare as a danger to national security as well as a potential assault platform.[28] The US Cyber Command is in charge of centralising command of cyberspace operations, organising existing cyber resources, and coordinating protection of US military networks. It is a unified combatant command of the armed forces. The United States was named the world's leading cyber superpower in a 2021 study by the International Institute for Strategic Studies, based on its cyber-attack, defence, and intelligence capabilities.[29]

Former US President Donald Trump promised shortly following his campaign victory that he would present a comprehensive plan to strengthen US cybersecurity within 90 days of taking office.[30] He signed an executive order three weeks after the 90-day deadline, calling for the strengthening of the resilience of government networks.[31] According to the new executive order, federal agency heads will be held accountable for network breaches, and federal agencies would consolidate risk management processes using the National Institute of

[27] *IGCC, Lindsay, Jon, April 2012 China/Cybersecurity*, http://www.bdo3c.f-sc.org/archives/921.pdf.
[28] Grenoble, Ryan "Trump Reverses Obama-Era Rules on Cyberattacks". HuffPost.
[29] "Cyber Capabilities And National Power: A Net Assessment". *IISS*, 2021, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.
[30] "Nonexistent Trump cybersecurity policy worries experts - The Parallax". The Parallax. 23 March 2018.
[31] ibid

Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity.[32] In addition, within 90 days, federal departments were to assess their agencies' cyber security capabilities, concentrating on "risk mitigation and acceptance options" as well as assessing financial and technology sharing needs between departments. Cybersecurity experts later said that the order was "unlikely" to have a significant impact.[33]

President Trump signed the National Cyber Policy in September, which he described as "the first fully stated cyber strategy for the United States since 2003."[34] National Security Advisor John Bolton claimed in September 2018 that the Trump government's new "National Cyber Strategy" has supplanted restrictions on the use of offensive cyber activities with a legal regime that allows the Department of Defense and other appropriate authorities to penetrate foreign networks with greater authority to deter hacks on US structures. Bolton described the new approach as an effort to "build robust deterrent mechanisms that convince the enemy not to strike in the first place," adding that decision-making for strikes will be pushed down the chain of command rather than requiring presidential permission.[35]

In a September 2018 policy paper, the Department of Defense stated that it will "defend forward" US networks by stopping "malicious cyber activity at its source" and attempting to "ensure there are repercussions for reckless cyber action" by "keeping peace through strength."[36]

The National Cyber Strategy has also been criticised for being vague in judging actions and attempts of cyberwarfare against the United States, since existing US legislation does not specify what constitutes illegal cyber conduct that goes beyond what is permissible computer activity. Most information security research is controlled under the 1986 Computer Fraud and Abuse Act, which has been condemned for being "poorly written and arbitrarily applied" by allowing the prosecution of effective information security research methodologies. Top-level information security specialists are finding it difficult to enhance the cyber defense architecture as even necessary services are prohibited.[37]

In June 2010, Iran's nuclear plant in Natanz was attacked by the cyber-worm 'Stuxnet,' which is believed to be the most complex piece of malware ever identified and raises the prominence of cyberwarfare substantially.[38] In line with several assessments, it "put back Tehran's atomic programme by at least two years by destroying over 1,000 nuclear centrifuges."[39]

Despite a lack of formal confirmation, Gary Samore, Coordinator for Arms Control and Mass Destruction Weapons of the White House, issued an open statement stating, "We are delighted they have difficulties in using their centrifuge machinery and that we — the United States and its allies — are doing all we can to ensure that we complicate things for them."[40]

Comparative study

When comparing the cyber policies pursued by China and the United States to protect their economic and military interests, one can see differences in attitudes toward ownership (public versus private, the value of IP rights, and understandings of the value of intangible assets in general), control (restrictive versus democratic, the role of the state, the role of markets), and sharing (circumstances under which information sharing leads to

[32] "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure | The White House". whitehouse.gov.
[33] Ibid
[34] "President Trump Unveils America's First Cybersecurity Strategy in 15 Years | The White House". whitehouse.gov. 20 September 2018.
[35] Groll, Elias. "Trump Has a New Weapon to Cause 'the Cyber' Mayhem". Foreign Policy.
[36] "President Donald J. Trump Is Strengthening America's Cybersecurity". whitehouse.gov.
[37] Wheeler, Tarah. "In Cyberwar, There are No Rules". Foreign Policy.
[38] AFP: Stuxnet worm brings cyber warfare out of virtual world. Google.com (1 October 2010).
[39] Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon | Video on. Ted.com.
[40] Gary Samore speaking at the 10 December 2010 Washington Forum of the Foundation for Defense of Democracies in Washington DC, reported by C-Span and contained in the PBS program Need to Know ("Cracking the code: Defending against the superweapons of the 21st century cyberwar", 4 minutes into the piece)

positive sum, negative sum, and zero-sum outcomes). These disparities largely derive from a combination of political system characteristics, political-economic features, and economic development levels, as well as historical reasons, including strongly-held attitudes about risks and vulnerabilities.

In many situations, online risks are poorly allocated. Perfect security is impossible to achieve, but even if it were, it would be undesirable. The trade-off between security, efficiency, and liberty also means that there is a persistent degree of insecurity, where the advantages of efficient operations outweigh any risk reductions caused by additional security measures. There is a scarcity of useful data in the security arena to drive security investment. One reason why accurate estimates of information security losses are difficult to come by is because victims sometimes have a motive to under-report events. Unreliable data can take various forms, ranging from security vendors exaggerating cybercrime losses to continuous warnings of digital Armageddon caused by the exploitation of process control system vulnerabilities while obstructing discussion of actual or attempted assaults.[41] The existence of an information asymmetry does not imply that society is not spending enough on security or that it is allocating too much money. Rather, it suggests that it is unlikely to invest in the appropriate defenses in the appropriate proportion. Furthermore, the behaviour in the digital domain is inherently shaped by a wide range of externalities, wherein one person's activities have unintended consequences for others.

Each of these economic hurdles is expected to affect China. However, there are certain distinctions that might be used as a foundation for cross-country comparisons. First, the motivations of Chinese stakeholders may differ. The information security business is dominated by companies from the United States and Europe. As a result, there may be less incentive conflict for China to support policies that increase information security, even if they threaten the security industry's economic models. Security organisations, for example, have been shown to be hesitant to share data about security events and threats, even when doing so may significantly enhance overall security. Even if the West refuses, China may be prepared to encourage collaboration on exchanging security information. Second, externalities may be regarded in China in a very different way than they are in the West.[42] A useful embedded case study in this regard is industrial espionage. Losing trade secrets via hacked systems is obviously an undesirable outcome from the victim's standpoint. To the perpetrator, though, this represents a gain. As a result, determining whether the broad susceptibility of the world's computers provides net advantages or damages is increasingly challenging. If China has developed an industrial strategy that encourages or at least tolerates conducting espionage on behalf of its own businesses, the benefits to China must be evaluated against the susceptibility of Chinese Internet users whose machines may become infected and inflict harm.

Because of policy deadlock and fear of harming Internet efficiency, policy interventions (safety regulations, software liability, indirect intermediary liability, public–private partnerships, information disclosure requirements, cyber insurance) are likely to remain light-touch and hands-off in Western countries. In critical infrastructure sectors, voluntary information disclosure and public–private partnerships are favoured, maybe in combination with some safety legislation. When developing its own information security rules, China may choose to adopt a combination of these techniques. There may, however, be chances to test solutions that are unlikely to acquire momentum in the West. While software liability is unthinkable in most Western countries, it might theoretically be used in China, which lacks a robust software sector. This might be a helpful contrast to other nations' more laissez-faire policies.

Cybersecurity is also a top issue for governments around the world, including the United States and China, as well as information technology companies. All firms desire a safe digital infrastructure for commercial transactions, and technology companies are especially motivated to design and incorporate security into the DNA of their products and systems to assure the infrastructure's continuing viability and development. Governments, on the other hand, want a safe global digital infrastructure for economic development, efficiency,

[41] "Security Vs. Liberty? Is There A Trade Off?". *E-International Relations*, 2021, https://www.e-ir.info/2011/06/23/security-vs-liberty-is-there-a-trade-off/.
[42] *Uscc.Gov*, 2021, https://www.uscc.gov/sites/default/files/2020-08/June_24_2020_Hearing_Transcript_0.pdf.

and security. Over the last 6-12 months, both Congress and the Administration in the United States have proposed an increasing number of policy recommendations relating to cybersecurity. The Senate and House of Representatives have introduced a number of legislative measures.[43] Despite heated discussion, however, none of these bills have passed or become signed into law – and they are unlikely to do so in the near future, given the increasingly political tone around cybersecurity and parliamentary stalemate. While the technology sector almost overwhelmingly support Congressional action on specific topics that will demonstrably improve information security sharing on cyber threats, reform of the Federal Information Security Management Act (FISMA), cybersecurity research and development (R&D), enhanced penalties for cybercrime, and a national data breach standard – the industry as a whole has a less unified position. Industry fears an overly regulated strategy that is centred on the United States, which would fragment cyberspace and reduce security.

China has also suggested or adopted stringent regulatory cyber-related policies. Foreign encryption technology is restricted or outright prohibited under the 1999 encryption legislation.[44] 13 technological product categories need to undergo severe certification procedures for sale in China under the China Compulsory Certification for Information Security ("CCCi"), albeit only for government purchase. According to the Multi-Level Protection Scheme (MLPS), information security goods supplied into systems rated "3" or above must incorporate Chinese indigenous IP, and products sold into all system levels must comply with a slew of underlying requirements.[45]

When taken collectively, these regulations have the potential to drastically reduce the universe of technologies accessible in our marketplaces. This would stymie our governments' and companies' capacity to react to emergent, borderless cyber threats such as online crime, fraud, and theft. In addition, it will stifle indigenous innovation. Because security underlies the usage of the Internet and e-commerce, the end effect is a global slowdown in economic progress. Both governments should seek cybersecurity regulations that provide the necessary levels of security to address national security concerns while maintaining interoperability, openness, and a global market, according to the technology industry.

V. Conclusion

It is frequently stated that the road to hell is paved with good intentions. While there are numerous promising ideas for de-confliction and de-escalation in cyberspace, China and the US have gone through and will likely continue to undergo periods of intense friction as a result of a series of policies and actions taken by their governments to enact their sovereignty and endorse their respective strategic interests. However, at the most fundamental level, all sides have a shared interest in successfully managing and controlling their disputes, avoiding military confrontations, and fostering a more stable international environment. Serious military confrontation might be sparked by friction in emerging security areas, such as space and cyberspace, as well as conventional security concerns in hotspot regions.

Deriving from this analysis, this paper turns to articulating the need for both parties to make reciprocal goodwill gestures for stability in the cyber domain. To further this objective, the US is likely to move toward acknowledging and adapting to, in some form, China's idea of cyber sovereignty, therefore satisfying China's principal concern about internal stability. To be more specific, the US contribution would be to respect the Chinese government and people's wishes for domestic cyberspace governance. In exchange, the US may expect China to reciprocate its goodwill by agreeing to follow a different set of rules regarding international cyber normative frameworks, and its cyber behaviour toward the US in particular.

In practice, the US would not condone but would openly acknowledge China's right to use what is now a fairly extensive cyber surveillance programme internally in the purpose of preserving domestic stability, as currently established. For its part, China would explicitly accept (though not necessarily endorse) the United States' use of

[43] *IGCC, Lindsay, Jon, April 2012 China/Cybersecurity* http://www.bdo3c.f-sc.org/archives/921.pdf.
[44] Diplomat, The. "China'S Cybersecurity Law: What You Need To Know". *Thediplomat.Com*, 2021, https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/.
[45] ibid

its own vision of international cybersecurity and self-defence in both peacetime and wartime. This would necessitate China to be sensitive and receptive to US cyber sovereignty concerns by taking far more proactive measures to enforce its policy of prohibiting and punishing any party from using Chinese territory, to conduct cyber-attacks against the US (and many others), and to recognise that the use of cyber weapons in wartime would be controlled by the same rules applied to the use of other armaments.

Such agreements are compatible with both countries' individual and shared fundamental interests in and beyond cyberspace. Such accords would be extremely beneficial to the international community, exactly as Xi predicted at the 19th Communist Party Congress. True to Lao Tzu's renowned saying, "the journey of a thousand miles begins with a single step,"[46] Xi has already taken the first brave step in this regard with his historic 2015 cyber agreement with Obama. It is finally time to take the next step in cyberspace.

References

i. *IGCC, Lindsay, Jon, April 2012 China/Cybersecurity*, http://www.bdo3c.f-sc.org/archives/921.pdf.
ii. "Edward Snowden: Leaks That Exposed US Spy Programme". *BBC News*, 2021, https://www.bbc.com/news/world-us-canada-23123964
iii. Jinghua, Lyu. "What Are China'S Cyber Capabilities And Intentions?". *Carnegie Endowment For International Peace*, 2021, https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734
iv. Roberts, Huw et al. "The Chinese Approach To Artificial Intelligence: An Analysis Of Policy, Ethics, And Regulation". AI & SOCIETY, vol 36, no. 1, 2020, pp. 59-77. Springer Science And Business Media LLC, doi:10.1007/s00146-020-00992-2. Accessed 10 Sept 2021
v. G, Suresh. "Https://Medwinpublishers.Com/NNOA/NNOA16000183.Pdf". *Nanomedicine & Nanotechnology Open Access*, vol 5, no. 2, 2020. *Medwin Publishers*, doi:10.23880/nnoa-16000183.
vi. Chen Zhou, "A Review of China's Military Strategy," China Armed Forces 1:1: 19.
vii. Lin Cheng-yi, "China's 2008 Defence White Paper: The view from Taiwan," China Brief IX:3: 14.
viii. James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," 257
ix. Timothy L. Thomas, "Nation-state Cyber Strategies: Examples from China and Russia," in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (eds.), Cyber- power and National Security (Dulles, VA: Potomac Books, Inc. and NDU Press, 2009), 468; James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," 258.
x. Stratfor, "China: Pushing Ahead of the Cyberwarfare Pack," September 2, 2021, avail- able at: http://tinyurl.com/5u6j4qc (www.stratfor.com/memberships/132785/ analysis/20090225_china_pushing_ahead_cyberwarfare_pack).
xi. Qiao Liang and Wang Xiangsui, Unrestricted Warfare, Beijing: PLA Literature and Arts Publishing House, 1999, 29, 47, 211–212.
xii. David Leppard, "China bugs and burgles Britain," Times Online, available at: http://www.timesonline.co.uk/tol/news/uk/crime/article7009749.ece.
xiii. John F. Burns, "Britain Warned Businesses of Threat of Chinese Spying," New York Times, available at: http://www.nytimes.com/2010/02/01/world/europe/01spy.html.
xiv. Siobhan Gorman, "Electricity Grid in U.S. Penetrated by Spies," Wall Street Jour- nal, available at: http://online.wsj.com/article/SB123914805204099085.html.
xv. "Cyber spies assault US power grid," Jane's Intelligence Digest. Simon Tisdall, "Cyber-warfare 'is growing threat,'" Guardian, available at: http://tinyurl.com/ylav6sg (www.guardian.co.uk/technology/2010/feb/03/ cyber-warfare-growing-threat); and Kate Connolly, "Germany accuses China of industrial espionage," Guardian, available at:

[46] "Xi Outlines Blueprint to Develop China's Strength in Cyberspace," Xinhua, Accessed September 16, 2021, http://www.chinadaily.com.cn/a/201804/21/WS5adb0909a3105cdcf6519b2c.html.

http://tinyurl.com/n7ggep (www.guardian.co.uk/world/2009/jul/22/ger- many-china-industrial-espionage).

xvi. "U.S. Steps Up Effort on Digital Defenses," New York Times.

xvii. "Total gridlock—Cyber threat to critical infrastructure," Jane's Intelligence Review

xviii. "Cyber spies assault US power grid," Jane's Intelligence Digest.

xix. U.S.-China Economic and Security Review Commission (USCC), 2009 Report to Congress of the U.S.-China Economic and Security Review Commission, 167; "U.S.: Cyberspies Attack Joint Strike Fighter Project—Report," Stratfor, available at: http://tinyurl.com/655lbou (www.stratfor.com/memberships/136342/sitrep/20090421uscyberspiesattackjointstrikefighterprojectreport)

xx. "Computer Spies Breach Fighter-Jet Project," Wall Street Journal

xxi. Grenoble, Ryan "Trump Reverses Obama-Era Rules on Cyberattacks". HuffPost.

xxii. "Cyber Capabilities And National Power: A Net Assessment". *IISS*, 2021, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

xxiii. "Nonexistent Trump cybersecurity policy worries experts - The Parallax". The Parallax. 23 March 2018. Accessed 16th Sept, 2021

xxiv. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure | The White House". whitehouse.gov.

xxv. "President Trump Unveils America's First Cybersecurity Strategy in 15 Years | The White House". whitehouse.gov. 20 September 2018.

xxvi. Groll, Elias. "Trump Has a New Weapon to Cause 'the Cyber' Mayhem". Foreign Policy.

xxvii. "President Donald J. Trump Is Strengthening America's Cybersecurity". whitehouse.gov.

xxviii. Wheeler, Tarah. "In Cyberwar, There are No Rules". Foreign Policy.

xxix. AFP: Stuxnet worm brings cyber warfare out of virtual world. Google.com (1 September 2021).

xxx. Ralph Langner: Cracking Stuxnet, a 21st-century cyber weapon | Video on. Ted.com.

xxxi. "Security Vs. Liberty? Is There A Trade Off?". *E-International Relations*, 2021, https://www.e-ir.info/2011/06/23/security-vs-liberty-is-there-a-trade-off/.

xxxii. *Uscc.Gov*, 2021, https://www.uscc.gov/sites/default/files/2020-08/June_24_2020_Hearing_Transcript_0.pdf.

xxxiii. Diplomat, The. "China'S Cybersecurity Law: What You Need To Know". *Thediplomat.Com*, 2021, https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/.

xxxiv. "Xi Outlines Blueprint to Develop China's Strength in Cyberspace," Xinhua, Accessed September 16, 2021, http://www.chinadaily.com.cn/a/201804/21/WS5adb0909a3105cdcf6519b2c.html