ACIG
APPLIED
CYBERSECURITY
& INTERNET
GOVERNANCE

NASK

Collaborating Pariahs: Does the Ukraine War Cement an Adversarial Cyber-Information Bloc?

Chris Bronk | Hobby School of Public Affairs, University of Houston, USA |
ORCID: 0009-0002-6778-2206

Received: 20.01.2024

Accepted: 23.05.2024

Published: 28.06.2024

Cite this article as:
C. Bronk, “Collaborating pariahs: Does the Ukraine war cement an adversarial cyber-information bloc?,” ACIG, vol. 3, no. 1, 2024, DOI: 10.60097/ACIG/190263

Corresponding author:
Chris Bronk, Hobby School of Public Affairs, University of Houston, Houston, TX, USA. E-mail: rcbronk@Central.UH.EDU;
0009-0002-6778-2206

Abstract

Russia’s 2022 invasion of Ukraine has dramatically altered global politics, not least that several so-called pariah states appear to be cooperating at a deeper level than at any time since the end of the Cold War. Occupying a critical position between the pariahs and the rest of the community of nations is China, an adversary to the United States, but not a pariah to the degree of Russia or its allies North Korea and Iran. Each of these countries has advanced both cyber and information operations. Considered here is a framework for understanding linkages between China and the pariahs; a chronicle of cyberattacks by each of the countries mentioned as well as consideration of possible collaboration; and observations on their propagandistic information operations since the beginning of the Russo-Ukraine War.

Keywords

cybersecurity, information influence, role theory

Russia is a country, but Russia plus Ukraine is an empire.
– Zbigniew Brzezinski

1. An Axis of Adversaries

When George Bush coined the term *axis of evil* in his 2002 State of the Union address, we could hardly imagine the current bloc of authoritarian nation-states cooperating to subvert the international order in place since the end of the Cold War. Where it was difficult to see Iran, Iraq, and the Democratic People's Republic of Korea (DPRK or North Korea) as able to dramatically influence global events through cooperative action, two decades later China and Russia have cultivated international partners whose influence may be found from the Korean Peninsula to the Esequibo area of South America [1]. This has profound meaning for cyber conflict, online influence campaigns, and the development of sophisticated military technology. With its invasion of Ukraine on 24 February 2022, Russia joined Iran and North Korea in the world's club of pariah states [2].

Russia's general invasion of Ukraine in 2022 also represents *a new phase in cooperation between authoritarian nation-states*. Russia, Iran, and North Korea are not just reimagined rogues of the international system but rather representatives of a new international order of non-democratic nations. Each of these states has close relations with Xi Jinping's People's Republic of China [3]. This is not a rehash of the Soviet Union's Warsaw Pact but rather a group of autocrat-led countries which stress and strain the diplomacy and military power of Western countries referred to by some as 'NATO Plus' (NATO+). What these four countries have been able to do is to sow chaos through the threat of force or its employment around the globe. The Russo-Ukraine War has shown that Vladimir Putin's regime has friends, and those friends are willing and able to aid in the war effort. Iran supplies the inexpensive drones blasting Ukraine's energy infrastructure. North Korea exports artillery ammunition. China cleared boycotted Russian oil exports from the global market, albeit at a substantial discount.

In the wake of Putin's grab for Ukraine, the authoritarian states identified here have been rhetorically cooperative, but to what degree have their cyber and information influence operations intersected? For example, China allegedly launches information influence campaigns against Taiwan [4], employing lessons learned by Russia and where Iran makes use of cyberattack knowledge from North Korea [5]. Beyond that, these countries lay underpinnings of challenges of the Western order they perceive as operating against their interests. Presented here are: (1) a framework for describing the linkages between these four states, both before and after the 2022 Ukraine invasion; (2) the *modus operandi* of cyberattack by each as well as an appraisal of recent (last 24 months) activity; and (3) description of information operations in the form of digital propaganda, and how those operations have evolved since Russia attempted to capture Kyiv and gain control over Ukraine.

2. Framework: Autocratic Alignment and the Russo-Ukrainian War

Russia's invasion of Ukraine across several axes on 24 February 2022 represented both major escalation of their conflict dating back to 2014 and dramatic change in the international system. Competition between major powers, set aside during the period of US hegemony for the prior three decades, was firmly reinitialised. This has triggered a reappraisal of theoretical models for understanding international relations and foreign policy [6]. At the core of this analysis resides the question of how strategic linkages between several autocratic states may arise. Central to this thesis is a reimagined Russia willing to scuttle relations with its Western economic partners and double down on its cooperation with other autocratic regimes. Like others in the international system, Russia seeks security, although of late it appears more inclined to destabilise other states and undermine its near-abroad neighbours.

Putin's Russia is part of just one traditional security pact, the Collective Security Treaty Organization (CSTO), which includes five other Soviet successor states. It also has many defence cooperation agreements (DCAs), which are 'formal bilateral agreements that establish institutional frameworks for routine defence cooperation' [7]. Russia maintains DCAs with no less than 20 countries across the Americas, Africa, Asia, and Europe, including ones with China, North Korea, and Iran. Finally, there is the Shanghai Cooperation Organization (SCO), which includes China, Iran, and Russia, but not North Korea.[1] It sends mercenaries to the Middle East and Africa; sells arms to dozens of nations; and appears willing to share technology with its closest allies.

The 2022 invasion of Ukraine has moved Russia to the status pariah state [8]. What does that mean? 'Pariah states are ostracized by significant portions of the international community for egregiously violating international norms'. Typically, they are governed by 'insecure authoritarian regimes' [9]. As a pariah state, Russia joins a growing list of others, including Myanmar, Venezuela, and Syria as well as Iran and North Korea. It is much larger than any of the others, and its future is largely dependent upon a linkage to China. 'For pariah states that flout international norms, China is a key

[1] The SCO also includes both India and Pakistan, nation-states with great enmity for each other.

source of diplomatic and economic support'. For Russia, China's support is embodied in the actions of an enabling sponsor which aids in evading sanctions, performs the role of a diplomatic shield, and engages in supporting information operations [10].

2.1. A Renewed Sino-Russian Alliance?

The closeness of collaboration between China and Russia rests upon how much they see themselves as aligned against the United States and how much Xi's China is willing to cooperate with heavily sanctioned pariah regimes. There are several metrics to consider in Sino-Russian cooperation. In the last decade, Xi Jinping and Vladimir Putin have met 42 times [11]. These meetings have occurred following the invasion of Ukraine, with a bilateral visit in Moscow in March 2023, followed by a sideline visit at the Third Belt and Road Forum in Beijing. Then there is trade. In 2023, the volume of trade between Russia and China hit a record high of $240.1 billion, marking a 26.3% increase from the previous year [12]. The volume of Russian oil exports to China rose by 24%, making it China's largest crude oil supplier, ahead of imports from Saudi Arabia [13].

There are also the words that unite the pair. In the joint declaration made weeks before Russia's Ukraine invasion, Xi and Putin indicated a deepening of ties. Their statement made at the opening ceremony of the XXIV Olympic Winter Games reaffirmed 'the new inter-State relations between Russia and China are superior to political and military alliances of the Cold War era', and that 'friendship between the two States has no limits' [14]. In a December 2022 call between Xi and Putin, Xi reiterated the need for, 'China and Russia to remain true to the original aspiration of cooperation, maintain strategic focus, [and] enhance strategic cooperation' [15]. More than two years into the Russo-Ukrainian War, Putin and Xi continue to celebrate 'deepened bilateral engagement and cooperation' between their countries [16].

2.2. What Role Theory?

As the international system migrates away from US hegemony to a new period of competition between major powers, there is also a need to reappraise approaches to understanding power in international relations. As was true on the eve of the Second World War, we can assume that power is wielded in three major areas: military, economic, and information [17]. China, Russia, North Korea, and Iran, the Big Four of major US adversaries, all engage in significant cyber and information operations. The question for the immediate future is how much these countries may cooperate in those operations. This requires an analysis of academic and trade cybersecurity sources as well as information operation trackers. That said, we require a theoretical overlay for understanding how the rogue regimes studied identify themselves as individual *and* collective actors. For this, we need a theoretic construct for understanding the roles that those states choose to play and how they prioritize those roles.

Holsti's groundbreaking work on state roles may serve as a beneficial heuristic device for understanding the foreign policy of pariah state cooperation [18]. While not a major plank of international relations, role theory can be a form of bootstrapping construct for understanding state behaviour. It 'offers a framework for describing national role performance and role conceptions and for exploring the sources of those role conceptions' [18]. Although more than five decades have passed since role theory came to foreign policy analysis, others have found it to have utility. Walker made use of role theory in much of his scholarship, including a contribution produced with Malici, highly relevant to this thesis on role theory and the behaviour of rogue states [19]. Thies and Breuning considered how it may be used to bridge study of foreign policy and international relations [20]. Cantir and Kaarbo employed it in understanding how domestic politics shape foreign policy roles [21].

While the role definitions that Holsti devised speak to the time of conceptualisation at the mid-point of the Cold War, we can consider the roles China and its pariah allies as contemporary analogues. Iran conceives of itself as both a 'defender of the faith' and 'regional leader'. North Korea may be the best described as an 'anti-imperialist agent' and a 'faithful ally' of China. Finally, Russia, the newest member of the pariah club, may see itself in the roles of regional leader and protector as well as an agent standing against the West. Goodness of fit of contemporary behaviour to mature theory is undoubtedly fraught with the potential for mischaracterisation, but the question at hand is how to place cyber and information operations into a conception of role.

How do we assign roles to understand cyber and information operations? That is the fodder for the following two sections. We must examine how these states behaved before 24 February 2022 as well as after this date. First to be treated is the milieu of cyberattack, which can be generally described as the subversion of systems regarding their maintenance of confidentiality, integrity, and availability [22]. This is an area in which each of the four countries studied definitely have developed clear behaviours that may translate to broader state roles.

3. Cyber Operations

Fancy Bear, *APT 28*, *Lazarus Group* – these are the code names given by the Western cybersecurity industry to different groups subverting online systems for political and military purposes, often as part of a criminal enterprise more lucrative than the drug trade. Since Russia's full-scale invasion of Ukraine in February 2022, some consider cyber conflict eclipsed by kinetic forms of warfare [23]. When we look at how the core members of the adversarial bloc use cyber techniques, there is little of the kinetic cyberattack activity of the sort perhaps feared most, but the employment of cyberattack remains an important tool for our four major adversary states.

North Korea robbed the accounts of a foreign central bank. Iran likely erased thousands of computer hard drives at Saudi Arabia's national oil company. Russia figured for attempting to destroy the computers used to operate portions of Ukraine's power grid. China was labelled the greatest thief of intellectual property by former secretary of defense and CIA director Leon Panetta [24]. While any country able and willing appears to be using cyber methods for intelligence gathering, each of the states covered here also use them for what would be economic espionage or criminal activity; things shunned in the West. Each of the four powers identified here has brought unique attributes to cyber campaigns. In its cyber offensive behaviour, North Korea is a cybercriminal gangster state. Iran is a theocratic warrior mixing the efforts of proxies with cyber operations to destabilise its enemies. Russia has performed masterful cyber-espionage campaigns while also crossing the Rubicon into effective acts of cyber-kinetic action. Finally, China has used cyber techniques to vacuum up enormous amounts of sensitive and proprietary data while attempting to steer global data flows to its purview for purposes of surveillance and potentially subversion.

3.1. A Record of Cyber Exploits in Brief

Before the invasion of Ukraine, North Korea, Iran, Russia, and China had highly visible cyberattack programs of concern to the United States and its allies. North Korea stands out for its gangsterism as well as criminal cleverness. Kim Jong-Un's cyber forces are a state criminal enterprise, and they are expert in theft. As of 2022, North Korean hackers had reputedly stolen some $1.5 billion in cryptocurrency from the wallets of unsuspecting virtual currency holders [25]. In February 2016, North Korean hackers attempted an enormous heist, attempting to lift nearly $1 billion from the Bangladeshi central bank's account at the New York Federal Reserve Bank. North Koreans are also behind a significant piece of the global ransomware racket, with the country's *Lazarus Group* behind the 2017 *WannaCry* ransom encryption software [26]. While WannaCry raked in very little, perhaps $1.5 million, the cost to organisations and individuals stricken by it amounted to billions, making it a significant disruptive attack [27]. In addition, *WanaCry* made use of source code from a cyber exploit know to and used by the US Intelligence Community. Other North Korean cyber actions have aimed more at disruption adversaries than anything else.

Where North Korea's cyber efforts are largely designed to fill the coffers of state and its ruling elite, Iran has employed forms of cyber action to pursue its political–ideological objectives [28]. Important in understanding Iran's own offensive cyber aims is the impact of *Stuxnet*, a series of cyberattacks upon the country's nuclear-enrichment infrastructure. Discovery of the *Stuxnet* software did allow Iran to engage in an interesting form of collaboration. While most of the detective work on *Stuxnet* was performed by cybersecurity firms and experts, further investigation of Iran's sensitive networks revealed the presence of other sophisticated malware created by what was labelled *The Equation Group*, a euphemism for the US National Security Agency. The malicious software, codenamed *Duqu* and *Flame*, were discovered in a shared effort undertaken by Russian cybersecurity firm *Kaspersky* in collaboration with Budapest University of Technology and Economics as well as the Iranian national computer emergency response team (CERT). Iran found the International Telecommunications Union (ITU) a helpful partner in bringing *Flame* out of the shadows. The ITU's then director, Hamadoun Touré, is a graduate of Soviet graduate institutions, and may have aided cooperation between the parties to a considerable extent [29]. By focusing on Iran's compromised systems, Russia likely gained deep knowledge of the US and likely Israeli cyber operations and tools. Months after discovering *Flame*, Iran ostensibly launched *Shamoon*, a data deletion attack against its neighbour Saudi Arabia, targeting the country's national oil company [30]. Was it helped by Russia? That is a question without a publicly known answer.

Moving along to Russia, the rump state of the former Soviet Union has a record of cyber operations stretching back to the massive virtual attack it conducted against Estonia in 2007 [31]. Moscow launched increasingly sophisticated cyberattacks on Ukraine after the country's leadership chose to forge closer ties with the West. Those attacks became increasingly menacing after Russia's proxy operations in the Donbas and later invasion of Crimea. The *Petya/Not Petya* wiper malware spilled beyond Ukrainian targets, damaging the IT systems of several major multinational firms [32]. It also took a page from the *Stuxnet* playbook in its attempt to knock offline Ukraine's *oblenegro* regional electricity distribution concerns. While largely unsuccessful, this last operation struck a nerve as the Main Directorate of the General Staff of the Armed Forces of the Russian Federation, or GRU, demonstrated a significant capability in attacking industrial control system computers managing pieces of Ukraine's critical infrastructure [33]. Cyber operations, mostly designed to purloin sensitive information, were also a significant portion in Russia's information operations aimed at sowing chaos in the 2016 US national elections [34].

In stark contrast to Russia's disruptive operations, China's cyber activity has largely focused on one activity, espionage. China's cyber operations have vacuumed up massive amounts of information, largely in the areas of industrial espionage and the theft of intellectual property for both civilian and military development [35]. Google left China in 2010 over the theft of the firm's intellectual property via cyber means [36]. Chinese intelligence operatives penetrated the computer networks of the US Office of Personnel Management (OPM), the human resources office of the American government, and then proceeded to copy a massive volume of sensitive information on federal employees, including security clearance paperwork [37]. Elements of US weapons design have showed up repeatedly on Chinese platforms, indicating breaches at major defence contractors [38]. In addition to the collection of economic and military information, China has used cyber techniques for espionage directed at dissenters in its overseas diaspora, foreign diplomatic missions, and even the international organisations charged with regulating sport [39]. While often discovered in the act, China has remained undeterred in its massive cyber intelligence operation.

3.2. Activity in the Wake of the War(s)

How have the cyber operations of North Korea, Iran, Russia, and China changed in the last 2 years? To answer this, requires visits to the literature of cyberattack produced by cybersecurity companies, academics, and independent researchers. Ostensibly a failure of government in the United States and elsewhere, the cybersecurity industry provides an enormous amount of intelligence information regarding cyberattack techniques, hostile actors, and system vulnerabilities [40]. The actions of hostile states have evolved; however, each of the four countries studied appears to be sticking with its pre-2022 cyber operations gameplan. As the cybersecurity consultancy Crowdstrike demonstrates with its stockpile of incident response data (see Tab. 1), each of the four has largely stuck to its previously established pattern of attack behaviour.

That said, Iran's activity appears to have grown notably, not in the last 2 years, but more recently. Iran, once allegedly targeted by Israel for cyberattack, is increasingly turning the tables on it. Since the 7 October 2023 surprise attack by *Hamas* on Israeli territory adjacent to the Gaza Strip, Iran has dramatically increased its cyberattack activity. Operations include data leaks, data deletion, denial of service, and perhaps most menacing, threat of attack on critical infrastructure targets. Iran's cyber offensive capabilities are likely growing but examples of Iranian collaboration with other states remain few. In December 2023, Iran's legislature approved an agreement signed by the two countries' foreign ministers regarding cyber threats and information security [41]. Lopez-Rodriguez et al.

Table 1. Cyber activity by country, 2023.

Adversary group	Description
Russia	
Fancy Bear	Credential collection on MS-Exchange and phishing
Cozy Bear	Credential collection through MS Sharepoint and Office365
China	
Jackpot Panda	Malicious utility Trojan deployment
Cascade Panda	Actor-in-the-middle attacks & remote access tools (RAT)
North Korea	
Labyrinth Chollima	Supply chain compromise
Iran	
Spectral Kitten	Leaked PII, CCTV intrusions
Haywire Kitten	Cyber-kinetic attack threats, hack and leak ops, and distributed denial-of-service (DDoS)
Banished Kitten	Wiper data deletion attacks
Vengeful Kitten	Wiper and cellular infrastructure attacks

Source: Crowdstrike Global Threat Report 2024.

offer that both Russia and Iran have attacked energy infrastructure by cyber means but provide no evidence of collaboration in the wake of the Ukraine invasion [42]. Ties between Iran's increasing cyber attack profile and Russian support are rumoured, but thus far concrete evidence of those ties does not appear to have made it into open sources [43]. In messaging, however, there may be suggestions of greater closeness between China and its pariah allies.

4. Digital Propaganda

All four of the adversary states observed here have a two-fold information strategy. First and foremost, each maintains internal information controls on their populations [44]. To Western observers with relatively unfettered access to information, the internal information resources of Russia or China appear draconian. Regarding external information operations, the public messaging of state organs, especially Russia's, appear ludicrous. Of Ukraine, Russia's *Pravda* offers headlines like 'Zelensky's give-me-more-money ship is to sink at Davos' and 'Special military operation to end with Russia reuniting with Ukraine'. China's *People's Daily* suggests that American support for Ukraine equates to a message on how 'US pursuit of democracy puts world at risk'. Concern is that external propaganda strategies draw on this unreality to manipulate and subvert opinion in democratic states, in some cases with significant success. Internal and external information strategies of China and the pariahs combine unreality on both sides of the coin.

Internal controls on speech are common to the authoritarian regimes covered here. Massive powerful internal security forces are also common to all four countries. In Iran, its *Gast-e Ersad* or Guidance Patrol polices on violations of Islamic law while many of the other law enforcement agencies work to stifle counterrevolutionary activities [45]. North Korea also maintains an enormous, coercive internal security machine, which according to the US State Department human rights reporting may jail as many as 120,000 of the country's citizens [46]. Both Russia and China imprison political dissidents, protestors, and critics of their regimes. In both countries, dissidents frequently disappear, and China's government frequently purges government officials at the highest levels [47]. When former Chinese deputy leader Li Keqiang died in October 2023, aged 68, critics of the Chinese government wondered if his death by heart attack in a swimming pool was a euphemism as much as Russian deaths from falling out of windows [48].

With its massive information and computing technology (ICT) sector, China has thoroughly connected itself to the world's communications networks [49]. Conversely, access to the Internet in North Korea is highly restricted and limited primarily to government officials, select institutions, and a small number of foreigners living in the country. Most North Koreans do not have access to the global Internet, although some internal information technologies exist [50]. In between them reside Russia and Iran, both of which have purchased Chinese technologies that are part of its the so-called *Great Firewall* [51]. The *Great Firewall* is a sophisticated system for deep packet inspection and censorship of information access and communications [52]. In addition to blocking Internet traffic, China also employs a strategy to substitute Chinese-owned Internet platforms and tools for those owned by the US or Western firms. Facebook, Wikipedia, and X (formerly Twitter) are banned in China, and Internet searches are performed in compliance with China or not at all.

With the late 2021s, China brought its own applications to global audiences. In 2022, TikTok, a Chinese short-form video social media platform was again the most popular app download, globally, for mobile phones. This has drawn concern from Western governments [53]. TikTok is banned on the mobile devices of state employees in Texas, including the author. That said, the threat TikTok presents, other than to other forms of media, remains vague at best [54]. Other methods of Chinese propaganda range from state-run online news and entertainment to use of Western platforms for the placement of Chinese state messages and images [55]. Indeed, Chinese employment of social media in propaganda capitalizes on the US firms and their advertising business models [56].

It was Russia which showed how much the social media enterprise could be used to bring chaos to the lifeblood of the West's democratic governments, their elections. Nearly a decade after the US 2016 presidential election, considerable scholarship has been generated on how Russia employed social media to damage the political campaign of the candidate it found threatening, that of former senator and secretary of state Hillary Clinton [57]. Nadler et al. point out how the social media influencing technologies create a Digital Influence Machine (DIM), which can be employed, 'to identify and target weak points where groups and individuals are most vulnerable to strategic influence' [58]. As societies cultivated cultural and ideational influencers, Russian propagandists adapted their own influence techniques to this new, informational tableau for the purpose of achieving their external political goals. Zuboff's ‘surveillance capitalism’ had found a place in democratic politics [59]. The US social media firms were prepared to sell political advertising to firms they knew little or nothing about. Even worse, unlike traditional media, Facebook and Twitter held firm that they needn’t label political advertising with the source of the ad.

While 2016 may represent the high-water mark for digital subversion of electoral processes through malicious employment of social media, its use has broadened and continuing. China has now gradually increased its use of social media disinformation strategies. During the recent 2024 Taiwanese elections, it on social media actively attempted to support its favourites and discredit candidates it views as threatening [60]. This was part of a coercive strategy that also includes military and economic planks for bringing Taiwan under increasing Chinese control and eventually unifying it with Beijing. At the same time, Russia continues to use DIM strategies to drive a wedge between Ukraine and her foreign allies as well as undermine democratic politics in those states it finds to be most threatening to its own geopolitical ambitions [61]. Iran too, actively engages in online disinformation campaigns, especially in support of its proxy operations in Lebanon, Syria, and Yemen [62].

In contemporary stocktaking, the pariah states may be able to significantly influence the politics of countries at a global distance. Moscow and Beijing’s chief South American ally, Venezuela, has received strong informational support as its government postures to invade the oil-rich region of its neighbour Guyana [63]. Iran continues to produce propaganda in support of its Houthi and Hezbollah allies. For Russia and China, cooperation comes in the alignment of narratives and amplification of each other’s messages, especially on platforms like Twitter and Weibo [64]. Chinese state-controlled outlets help spread the Kremlin’s narrative of the war in Ukraine, often echoing Russian perspectives and criticisms of Western policies [65]. Additionally, both countries have targeted the Western financial system in their propaganda and disinformation campaigns. The collapse of Silicon Valley Bank in 2023, saw Russian and Chinese state media promoting narratives about the need for a new global financial system, often criticizing Western financial practices and institutions [66].

Iran presents again a novel picture for using the global information environment for its benefit. ‘Iranian cyber actors have been at the forefront of cyber-enabled I[nformation] O[perations], in which they combine offensive cyber operations with multi-pronged influence operations to fuel geopolitical change in alignment with the regime's objectives' [67]. But again, Iran's actions in digital propaganda have a lot less to do with events in Ukraine than its own regional ambitions and willingness to use cyber, information, or proxy operations to erode the standing of Israel, the United States, and others involved in the region. Microsoft's reporting on Iranian information influence operations in the wake of the 7 October 2023 attacks indicates a four-prong strategy on undermining Israel. First, it is releasing propaganda designed to polarise the Israeli public, often masquerading as left-leaning Israeli voices. Second, it makes threats to Israeli infrastructure, even if those threats can't be made good. Third, it has used email and text messages to damage the morale of Israeli defence forces and their families. Lastly, Iran has attempted to undermine international support for Israel by amplifying images of destruction and privation in Gaza [68].

The great unknown for information influence at the time of writing is how China and each pariah state will act during the 2024 US general election. No doubt much will happen and digesting the true meaning and intention of those events. Information influence does not take place in a vacuum. The US and its allies continue to mobilise effort to better understand how influence operations work and also on how they may be short-circuited. Are China, Russia, Iran, and North Korea cooperating on information operations or is it just that their operations share the same targets. This we will continue to learn with additional time and data.

5. Conclusions

Collective security has been the cornerstone of the West's international security policy since 1945 [69]. During the Cold War, the members of the Warsaw Pact either feared invasion by or were indeed invaded by the Soviet Union. Just as suddenly as Soviet control extended across the territories it occupied in Europe's East during the end and immediate aftermath of the Second World War, the Soviet Union collapsed with only a Russian rump state (and its nuclear arsenal) remaining. More than 30 years later, Russia has found new expansionist ambitions played out in its near abroad, most notably in its invasion of Ukraine. It now sits at the centre of a security arrangement with North Korea and Iran, two-thirds of President George W. Bush's *axis of evil*. The full-scale war in Ukraine since 2022 has made Moscow an importer of arms from those two countries by sheer necessity. These both countries are also escalating their positions in regional conflicts and proxy wars to make the job of Western diplomacy and defence markedly harder. This stretches an American defence establishment thinner at a time when the maintenance of the US conventional deterrence appears more difficult [70].

Where that deterrence may be most important for the moment is in the Western Pacific. China's cyber and information operations indicate a growing impatience with Taiwan's independent status. Fortunately for Taiwan, cyber and information operations are far easier to undertake than kinetic military operations. The fundamental question to be answered from the conjectures offered here is to what degree China is part of the informal alliance between Russia, North Korea, and Iran [71]. If it is, then that makes the geopolitical stage all that more dangerous. That is because China brings an economic strength that the pariah states do not have. Time will tell if the adversarial bloc is real or if significant distance remains between China and the rest. For the American consumer, China is the manufacturer of their shoes, clothes, laptops, computers, and other consumer goods. For the US defense planner, it is the prime threat to Asian security and the justification for a 'pivot to Asia' that begun in the Obama administration [72]. Rectifying these realities into a workable strategic vision is vexing to say the least.

There are limits to cooperation. China and each of the pariahs has its own parochial interests. While evidence of an ideological break may exist between the West and China, this does not necessarily translate to a fundamental military or economic one. With many Western democracies still importing Russian oil and gas, Moscow has avoided a full economic disconnect from the rest of the world despite its invasion of Ukraine. For China, its bellicose language over Taiwan, maritime disputes, and other issues have not translated to a disconnection of its economy from the rest of the world either. If there is a lesson to be learned, it is that rhetoric in the channels of information power rarely matches willingness to engage in economic or military conflict. Talk remains cheap and the Internet makes transmitting it even cheaper.

Will China go it alone in meeting its objectives? Despite its now mature Belt and Road initiative, Chinese lending and infrastructure development has not yielded the form of security relationships coveted in Washington – 'The United States has fifty security pacts with different countries around the world. China has only one, with North Korea' [73]. If Russia, North Korea, and Iran are now China's allies, they make Beijing's designs on territorial aggrandizement in the South China Sea and absorption of Taiwan more achievable, simply by distracting the United States and its allies. Combined, these four nation-states can make much chaos in the information environment and cyber domain. They also can tie down NATO+ assets with the mere threat of military action. How well they will hang together and work collectively towards shared goals is perhaps the most pressing question in international security today.

References

[1] M. Kaczmarski, "The Sino-Russian relationship and the West," *Survival*, vol. 62, no. 6, pp. 199–212, Dec. 2020, doi: 10.1080/00396338.2020.1851101.

[2] T. Lattmann, "From partner to pariah: The changing position of Russia in terms of international law," in *Russia's Imperial Endeavor and Its Geopolitical Consequences: The Russia-Ukraine War*, Volume Two, B. Madlovics, B. Magyar, Eds., New York, NY: Central European University Press, 2023, pp. 183–198.

[3] L. Yu, S. Sui, "China-Russia military cooperation in the context of Sino-Russian strategic partnership," *Asia Europe Journal*, vol. 18, pp. 325–345, 2020, doi: 10.1007/s10308-019-00559-x.

[4] J. Lewis. (Aug. 11, 2023). *Cyberattack on civilian critical infrastructures in a Taiwan scenario*, Center for Strategic and International Studies. [Online]. Available: https://www.csis.org/analysis/cyberattack-civilian-critical-infrastructures-taiwan-scenario. [Accessed: Dec. 7, 2023].

[5] S. Ragan. (Sep. 4, 2012). *Iran and North Korea Join Forces on Science and Technology*, *SecurityWeek*. [Online]. Available: https://www.securityweek.com/iran-and-north-korea-join-forces-science-and-technology. [Accessed: Nov. 03, 2023].

[6] A. Malici, S.G. Walker, *Role Theory and Role Conflict in US-Iran Relations: Enemies of Our Own Making.* Abingdon, Oxfordshire: Routledge, 2016.

[7] B. J. Kinne, "Defense cooperation agreements and the emergence of a global security network," *International Organization*, vol. 72, no. 4, pp. 799–837, 2018, doi: 10.1177/0022002719857796.

[8] K. Stoner, "The war in Ukraine: How Putin's war in Ukraine has ruined Russia," *Journal of Democracy*, vol. 33, no. 3, pp. 38–44, 2022, doi: 10.1353/jod.2022.0038.

[9] L.-E. Easley, J.T. Chow, "Enabling pariahs: China's support of Myanmar, North Korea, and Russia for geopolitical advantage," *Asian Survey*, vol. 64, no. 3, pp. 396–427, 2024, doi: 10.1525/as.2024.2113239

[10] J.T. Chow, L.-E. Easley, "Renegotiating pariah state partnerships: Why Myanmar and North Korea respond differently to Chinese influence," *Contemporary Security Policy*, vol. 40, no. 4, pp. 502–525, 2019, doi: 10.1080/13523260.2019.1660483.

[11] B. Lin, B. Hart, S. Lu, Y.-J. Liao. (Oct. 23, 2023.). *Analyzing the latest Xi-Putin meeting and China's belt and road forum*, Commentary, Center for Strategic & International Studies (CSIS). [Online]. Available: https://www.csis.org/analysis/analyzing-latest-xi-putin-meeting-and-chinas-belt-and-road-forum. [Accessed: Nov. 27,2023].

[12] Reuters. (Jan. 12, 2024.). *China-Russia 2023 trade value hits record high of $240 bln - Chinese customs*. [Online]. Available: https://www.reuters.com/markets/china-russia-2023-trade-value-hits-record-high-240-bln-chinese-customs-2024-01-12. [Accessed: Jun. 25, 2024].

[13] TASS Russian News Agency. (Jan. 19, 2024). *Russia exports record oil volume to China in 2023*. [Online]. Available: https://tass.com/economy/1734985. [Accessed: Jun. 25, 2024].

[14] President of Russia. (Feb. 4, 2022). *Joint statement of the Russian Federation and the People's Republic of China on the international relations entering a new era and the global sustainable development.* [Online]. Available: www.en.kremlin.ru. [Accessed: Nov. 27, 2023].

[15] R. Barrios, A. Bowen. (Sep. 13, 2023). *China-Russia relations*, Congressional Research Service, Washington, DC. [Online]. Available: https://crsreports.congress.gov/product/pdf/IF/IF12100. [Accessed: Nov. 27, 2023].

[16] W. Yang, "China, Russia double down on ties despite complications in trade relations," *Voice of America*, February 15, 2024.

[17] E.H. Carr, *The Twenty Years' Crisis, 1919-1939: Reissued with a New Preface from Michael Cox.* New York, NY: Springer, 2016.

[18] K.J. Holsti, "National role conceptions in the study of foreign policy," *International Studies Quarterly*, vol. 14, no. 3, pp. 233–309, 1970, doi: 10.2307/3013584.

[19] A. Malici, S.G. Walker, "Role theory and 'rogue states'," in *Deviance in International Relations: 'Rogue States' and International Security*. , W. Wagner, W. Werner, M. Onderco, Eds., London: Palgrave Macmillan, 2014, pp. 132–151.

[20] C.G. Thies, M. Breuning, "Integrating foreign policy analysis and international relations through role theory,"*Foreign Policy Analysis*, vol. 8, no. 1, pp. 1–4, 2012, doi: 10.1111/j.1743-8594.2011.00169.x

[21] C. Cantir, J. Kaarbo, "Contested roles and domestic politics: reflections on role theory in foreign policy analysis and IR theory," *Foreign Policy Analysis*, vol. 8, no. 1, pp. 5–24, 2012, doi: 10.1111/j.1743-8594.2011.00156.x

[22] O.A. Hathaway, R. Crootof, P. Levitz, H. Nix, "The law of cyber-attack," *California Law Review*, vol. 100, pp. 817, 2012.

[23] E. Roche, M. Blaine, "The folly of cyber war," *Journal of International Affairs*, vol. 75, no. 2, pp. 131–144, 2023.

[24] L. Panetta, B. Obama, *Sustaining US Global Leadership: Priorities for 21st Century Defense.* Washington, DC: US Department of Defense, vol. 1, p. 16, 2012.

[25] During a track two visit by North Korean diplomats to Syracuse University in 2000, the chief of the delegation asked the author several questions suggesting fairly strong knowledge of software design and computer coding: J. S. Wit. (2019). "U.S. strategy towards North Korea: Rebuilding dialogue and engagement". [Online]. Available: https://usakoreainstitute.org/wp-content/uploads/2010/02/NKreportOCT09jwit.pdf. [Accessed: Nov. 27, 2023].

[26] A. Greenberg, "North Korean hackers stole nearly $400 million in crypto last year," *Wired*, Jan. 13, 2022. [Online]. Available: https://www.wired.com/story/north-korea-cryptocurrency-theft-ethereum. [Accessed: Oct. 10, 2023].

[27] S. Mohurle, M. Patil, "A brief study of wanna cry threat: Ransomware attack 2017," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 5, pp. 1938–1940, 2017, doi: 10.26483/ijarcs.v8i5.4021.

[28] Web Titan. (Jul. 2, 2020). *How much money did wanna cry make?* [Online]. Available: https://www.webtitan.com/blog/how-much-money-did-wannacry-make. [Accessed: Dec. 03, 2023].

[29] G. Siboni, L. Abramski, G. Sapir, "Iran's activity in cyberspace: Identifying patterns and understanding the strategy," *Cyber, Intelligence, and Security*, vol. 4, no. 1, pp. 21–40, 2020.

[30] C. Bronk, "Cyber intrigue: The flame malware international politics," Cyber Dialogue, University of Toronto, May 31, 2012. [Online]. Available: https://cyberdialogue.ca/2012/05/cyber-intrigue-the-flame-malware-international-politics/. [Accessed: Nov. 03, 2023].

[31] C. Bronk, E. Tikk-Ringas, "The cyber attack on Saudi Aramco," *Survival*, vol. 55, no. 2, pp. 81–96, 2013, doi: 10.1080/00396338.2013.784468.

[32] C. Bronk, "Hacking the nation-state: Security, information technology and policies of assurance," *Information Security Journal: A Global Perspective*, vol. 17, no. 3, pp. 132–142, 2008, doi: 10.1080/19393550802178565.

[33] A. Greenberg, "The untold story of NotPetya, the most devastating cyberattack in history," *Wired*, Aug. 22, 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world. [Accessed: Nov. 27, 2023].

[34] R. Lee, M.J. Assante, T. Conway, "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, no. 388, pp. 1–29, 2016.

[35] C.E. Ziegler, "International dimensions of electoral processes: Russia, the USA, and the 2016 elections," *International Politics*, vol. 55, no. 5, pp. 557–574, 2018, doi: 10.1057/s41311-017-0113-1.

[36] N. Inkster, "Cyber espionage," *Adelphi Series*, vol. 55, no. 456, pp. 51–82, 2015, doi: 10.1080/19445571.2015.1181443.

[37] S.J. Hartnett, "Google and the 'twisted cyber spy' affair: US–Chinese communication in an age of globalization," *Quarterly Journal of Speech*, vol. 97, no. 4, pp. 411–434, 2011, doi: 10.1080/00335630.2011.608705.

[38] S. Gootman, "OPM hack: The most dangerous threat to the federal government today," *Journal of Applied Security Research*, vol. 11, no. 4, pp. 517–525, 2016, doi: 10.1080/19361610.2016.1211876.

[39] A. Gilli, M. Gilli, "Why China has not caught up yet: Military-technological superiority and the limits of imitation, reverse engineering, and cyber espionage," *International Security*, vol. 43, no. 3, pp. 141–189, 2018, doi: 10.1162/isec_a_00337.

[40] R. Deibert, R. Rohozinski, A. Manchanda, N. Villeneuve, G. Walton, *Tracking Ghostnet: Investigating a Cyber Espionage Network*. Toronto: Citizen Lab, University of Toronto, 2009.

[41] J.D. Work, "Private actors and the intelligence contest in cyber conflict," in *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*, R. Chesney, M. Smeets, Eds., Georgetown University Press, 2023.

[42] G. López-Rodríguez, I. Moreno-López, J.C. Hernández-Gutiérrez, "Cyberwarfare against critical infrastructures: Russia and Iran in the gray zone," *Applied*

Cybersecurity & Internet Governance, vol. 2, no. 1, pp. 1–7, 2023, doi: 10.60097/ACIG/162865.

[43] Iran International. (Dec. 10, 2023). *Iranian parliament approves information security deal with Russia.* [Online]. Available: https://www.iranintl.com/en/202312105187. [Accessed: Nov. 27, 2023].

[44] A. Davidi, "Iranian-Russian cooperation on hack attacks may challenge Israeli cyber supremacy," *The Times of Israel*, April 18, 2023.

[45] V. Weber, "The worldwide web of Chinese and Russian information controls," Oxford: Center for Technology and Global Affairs, University of Oxford, 2019. [Online]. Available: https://www.ctga.ox.ac.uk/article/worldwide-web-chinese-and-russian-information-controls. [Accessed: Jun. 25, 2024].

[46] S. Golkar, "The evolution of Iran's police forces and social control in the Islamic Republic," *Middle East Brief*, no. 120, vol. 3, pp. 1–9, 2018.

[47] K.C. Lee, "In the Kim Jong Un era what is the reality of social control and punishment in North Korea," *Korea Institute for National Unification*, 2023. [Online]. Available: https://repo.kinu.or.kr/handle/2015.oak/14464. [Accessed: Jun. 25, 2024].

[48] C. Chen, "What is behind anti-corruption? A comparison of Russia and China," *Communist and Post-Communist Studies*, vol. 53, no. 4, pp. 155–176, 2020, https://doi.org/10.1525/j.postcomstud.2020.53.4.155.

[49] K. Nakazawa. (Nov. 2, 2023). *Analysis: The mysteries and dangers that trail Li Keqiang's death*, Nikkei Asia. [Online]. Available: https://asia.nikkei.com/Editor-s-Picks/China-up-close/Analysis-The-mysteries-and-dangers-that-trail-Li-Keqiang-s-death [Accessed: Oct. 10, 2023].

[50] Y. Hong, G. T. Goodnight, "How to think about cyber sovereignty: the case of China," in *Norm Diffusion Beyond the West*, Š. Kolmašová, Ed. Springer Nature Switzerland, 2020, pp. 8–26.

[51] S.-A. Kim, C.Y. Kang, J. Park, B.Y. Yoon, *A Study on the Access to Information of the North Korean People*. Korea Institute for National Unification, 2021.

[52] S. Kalathil, *Beyond the Great Firewall: How China Became a Global Information Power*. Washington, DC: Center for International Media Assistance, 2017.

[53] E. Quan, "Censorship sensing: The capabilities and implications of China's great firewall under Xi Jinping," *Sigma: Journal of Political and International Studies*, vol. 39, no. 1, p. 4, 2022.

[54] A. Law, "The 'legal black hole' CFIUS and the implications of Trump's executive order against TikTok," *Cornell JL & Pub. Pol'y*, vol. 31, p. 217, 2021, doi: 10.59015/wlr.ACHH7075.

[55] M.L. Mueller, K. Farhat, "Regulation of platform market access by the United States and China: Neo-mercantilism in digital services," *Policy & Internet*, vol. 14, no. 2, pp. 348–367, 2022, doi: 10.1002/poi3.305.

[56] B. Min, L.R. Luqiu, "How propaganda techniques leverage their advantages: A cross-national study of the effects of Chinese international propaganda on the US and South Korean audiences," *Political Communication*, vol. 38, no. 3, pp. 305–325, 2021, doi: 10.1080/10584609.2020.1763524.

[57] J. Bund, *Finding China's Edge: Engineering Influence Operations within the Limits of Social Media Platform Rules*. ETH Zurich, 2021.

[58] Y. Golovchenko, C. Buntain, G. Eady, M.A. Brown, J.A. Tucker, "Cross-platform state propaganda: Russian trolls on Twitter and YouTube during the 2016 US presidential election," *The International Journal of Press/Politics*, vol. 25, no. 3, pp. 357–389, 2020, doi: 10.1177/19401612209126.

[59] A. Nadler, M. Crain, J. Donovan. (2018). *Weaponizing the digital influence machine*. [Online]. Available: https://datasociety.net/library/weaponizing-the-digital-influence-machine. [Accessed: Nov. 27, 2023].

[60] S. Zuboff, "The age of surveillance capitalism," in *Social Theory Re-Wired*, W. Longhofer, D. Winchester, Eds.,Abingdon, Oxfordshire: Routledge, 2023, pp. 203–213.

[61] H.-C. H. Chang, A. H.-E. Wang, Y. S. Fang. (2023). *US-Sskepticism: Misinformation and transnational conspiracy in the 2024 Taiwanese presidential elections*, Center for Open Science, [Online]. Available: https://misinforeview.hks.harvard.edu/article/us-skepticism-and-transnational-conspiracy-in-the-2024-taiwanese-presidential-election/. [Accessed: Nov. 27, 2023].

[62] L. Maschmeyer, A. Abrahams, P. Pomerantsev, V. Yermolenko, "Donetsk don't tell – 'hybrid war' in Ukraine and the limits of social media influence operations," *Journal of Information Technology & Politics*, pp. 1–16, 2023, doi: 10.1080/19331681.2023.2211969.

[63] H. Kermani, "#MahsaAmini: Iranian Twitter activism in the times of computational propaganda," *Social Movement Studies*, 2023, doi: 10.1080/14742837.2023.2180354

[64] R. Padula, M. de Freitas Cecílio, I. Candido de Oliveira, C.J. Prado, "Guyana: Oil, internal disputes, the USA and Venezuela," *Contexto Internacional*, vol. 45, 2023. [Online]. Available: https://www.scielo.br/j/cint/a/vTqm4rBBDg6WRMt3NyLyKtF/?format=pdf&lang=en. [Accessed: Jun. 25, 2024].

[65] S. Bendett, E. Kania. (2019). *A new Sino-Russian high-tech partnership," Australian Strategic Policy Institute*. [Online]. Available: https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership. [Accessed: Nov. 27, 2023].

[66] J. Bodnar, B. Schafer, E. Soula. (2023). *A Year of Disinformation: Russia and China's Influence Campaigns During the War in Ukraine*, Alliance for Securing Democracy. [Online]. Available: https://securingdemocracy.gmfus.org/a-year-of-disinformation-russia-and-chinas-influence-campaigns-during-the-war-in-ukraine/ [Accessed: Dec. 03, 2023].

[67] K. Walter, H. Hariharan, "China, Russia target western financial system with propaganda and disinformation," *The Diplomat*, Jul. 14, 2023. [Online]. Available: https://thediplomat.com/2023/07/china-russia-target-western-financial-system-with-propaganda-and-disinformation. [Accessed: Nov. 03, 2023].

[68] C. Watts. (May 2, 2023). *Rinse and repeat: Iran accelerates its cyber influence operations worldwide*. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2023/05/02/dtac-iran-cyber-influence-operations-digital-threat. [Accessed: Nov. 03, 2023].

[69] C. Watts. (Feb. 6, 2024.). *Iran accelerates cyber ops against Israel from chaotic start*. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel. [Accessed: Nov. 03, 2023].

[70] Charles. A. Kupchan, Clifford. A. Kupchan, “The promise of collective security,” *International Security*, vol. 20, no. 1, pp. 52–61, 1995.

[71] E.D. Borghard, S.W. Lonergan, “Deterrence by denial in cyber-space,” *Journal of Strategic Studies*, vol. 46, no. 3, pp. 534–569, 2023, doi: 10.1080/01402390.2021.1944856.

[72] N. Grajewski, “An illusory entente: The myth of a Russia-China-Iran ‘axis’,” *Asian Affairs*, vol. 53, no. 1, pp. 164–183, 2022, doi: 10.1080/03068374.2022.2029076.

[73] K.M. Campbell, R. Doshi, “How America can shore up Asian order,” *Foreign Affairs*, vol. 12, 2021. [Online]. Available: https://www.foreignaffairs.com/articles/united-states/2021-01-12/how-america-can-shore-asian-order. [Accessed: Jun. 25, 2024].

[74] D. Singh. (Jan. 18, 2024). *Déjà new: A return to the old normal. Security, economics, and technology for Houston Llecture*, University of Houston. [Online]. Available: https://www.law.uh.edu/ipil/2024_SETH_Lecture_Series_photos.asp. [Accessed: Nov. 27, 2023].