Journal on Baltic Security, 2023; 9(1): 1-31

Research Article

Open Access
https://doi.org/10.57767/jobs_2023_0002

Dries Putter and Sascha-Dominik Dov Bachmann *

Russia and China expected to renew their espionage vigour

Received: 16 January 2023
Accepted: 14 February 2023

Abstract: This article argues that both Russia and China will re-invigorate and expand their international espionage activities. Russia's renewed vigour in engaging in aggressive espionage campaigns is due to the current setbacks that it is facing as a result of its ill-fated invasion of Ukraine. The sanction-induced prohibitions that limit access to state-of-the-art technologies will unleash renewed enthusiasm to obtain these latest technologies by covert means, be it HUMINT and/or cyberespionage. The future robustness of China's aggressive espionage activities is projected to be fuelled by its systematic 'de-coupling' from those nations leading in science, engineering and technology, such as the United States, as well as the growing opposition to the use of developmental institutions such as the Confucius Institute and the Belt and Road Initiative (BRI) as intelligence collection platforms. This article predicts that as Russia and China become 'outsiders', they will becoming increasingly

* **Corresponding author:** Dr. Dries Putter, e-mail: putter@sun.ac.za. Senior Lecturer in Intelligence Studies at the Faculty of Military Science, Stellenbosch University Affiliate Member, National Security Hub, University of Canberra; Researcher, Security Institute for Governance and Leadership in Africa (SIGLA); Researcher, African Research Institute – Óbuda University, Hungary
Author: Prof. Sascha-Dominik Dov Bachmann, Professor in Law & Security and Co-Convener National Security Hub (University of Canberra), University of Canberra; Fellow Asia Pacific (Hybrid Threats and Lawfare) – NATO SHAPE; Research Fellow with the Security Institute for Governance and Leadership in Africa (SIGLA), Faculty of Military Science, Stellenbosch University.

aggressive in their espionage campaigns as pragmatic states acting in survival and developmental mindsets, and it elaborates on some of the more relevant forms of espionage employed.

Keywords: Russia, China, espionage, counterintelligence, national security

Introduction

Russia is currently experiencing a diplomatic ice-age of its own making due to its aggression against Ukraine and the ensuing war since 24 February 2022. Russia's national security is under severe pressure due to military strategic miscalculations, information blackouts, and increasing economic pressure. China is systematically being exposed as an aggressive imperialist regime, course-bound to challenge the extant world order and emerge as a superpower. Both of these nations have extended histories[1] of aggressive espionage to support their national ambitions. Walton retorted that 'part of the surprise and shock about recent revelations about Russian active measures, from poisonings in England to election meddling in the U.S., has arisen because of a lack of public understanding about their long history' (Pazzanese, 2019).

Rathbone and Jones write that 'Intelligence agencies have been slow to respond to the growing scope of covert Kremlin operations overseas' (Rathbone and Jones, 2022), inducing a sense of increased urgency within the Russian security services to conduct espionage against the West since the start of the Russo-Ukraine war (*Ibid.*). Five months after the start of the war, it was uncovered that Chinese state-sponsored cyber-threat groups are increasingly conducting cyberespionage on Russian organisations, based on findings by Sentinel Labs and the Google Threat Analysis Group (Coker, 2022). Western strategies aimed at keeping Russia and China strategically isolated to ensure that their exponential economic growth and imperialistic ambitions are

[1] See the summary for Richelson (1997) amongst a several other sources. Also, Faligot (2019).

stymied are fuelled by these developments. This is a key component that supports and enables Russian and Chinese ambition to grow and dominate is their aggressive appetite for espionage and consequently needs no introduction. From a pure theoretical perspective, such appetites are also supported by their realist approach to the international system, even self-defence could be argued, and some authors also argue for functionalist understanding (Baker, 2003; Konstantopoulos, 2012; Prochko, 2018). However, while international relations theories are useful to explain the behaviour of states, they tend to be less useful as a justification of such behaviour.

Increased Western efforts to expose Russia's and China's malign nationalist and revisionist ambitions raise awareness of key intelligence programmes leveraged by them. Their vast and inflated diplomatic networks, diaspora communities, and quasi-developmental economic programs are prime examples of how these countries stay informed, build capable espionage networks, and exercise foreign influence (Bachmann and Lee, 2020). With these increasingly being exposed, it can be expected that these countries will redouble their efforts to maintain and expand their foreign intelligence capabilities.

Since Russia's first bout of aggression against Ukraine and the subsequent invasion (CFR, 2022) in February 2014 (Bachmann and Gunneriusson, 2015), these national programs have been increasingly exposed for their true nature and labelled by various countries as threats to international and national security. Russia and China face the prospect of being systematically isolated from access to Western technology and opportunities to stymie uncontrolled expansion; their intelligence networks have been systematically dismantled by Western efforts. It would therefore not be unreasonable to predict an increased focus on espionage activities from these countries in the short-term to counter the escalating international push-back. Such a view is supported by the unprecedented joint FBI and MI5 statement on the expanding espionage threat from China (The Guardian, 2022).

Current and future espionage activities of any country are difficult to research academically due to the nature of the trade and national security implications. Thus, the researchers used open-source material from published media in support of their arguments. It would be extremely difficult to provide immediate evidence of such renewed enthusiasm due to the secret nature of this 'trade,' yet, however, the aim of the article is to highlight some of the significant setbacks that have been experienced by these two states vis-à-vis their abilities for intelligence collection. Based on these setbacks, the article projects that both Russia and China will be extremely busy in the short to medium term with efforts to repair damage to their intelligence networks and rebrand previously known initiatives, as well as to create new initiatives in support of their national ambitions and level some of their disastrous strategic miscalculations. The article will reflect on the role of Russia and China as increasingly outsiders in the international system due to their own strategic behaviour and then continue to highlight salient aspects that reinforce the contention of a future of heightened levels of espionage.

Russia and China - The Two Outsiders

Adm. Davidson (previously head of the US Indo-Pacific Command) testified before the US Senate Armed Services Committee that China poses the most significant 'long-term strategic threat' (FBI, 2020) to security and the rules-based international order in the 21st century. China is accelerating its ambition to replace the US as a global leader by 2050 (Starr, 2022). Both Russia and China have been labelled as the most serious threats to US national security from a subversion perspective (Kruger, 2020; FBI, 2020 and Star, 2022).[2] Similarly, the North Atlantic Treaty Organisation (NATO) finds both Russia and China to be the primary instigators and exploiters of 'political divergencies' amongst NATO members 'in ways that endanger their collective interests and security' (NATO, 2020). Such divergencies are typically exploited

[2] For perspectives on both Russia and China from a subversion perspective – which makes them prolific national security threats. This threat was already articulated by the FBI (2020) and more recently by Barbara Starr (2022).

through aggressive espionage targeting national security, science, engineering, and technology (SET) capabilities, as well as foreign influence operations and information operations.

Similarly, Russia and China are specifically associated with aggressive espionage programmes aimed at leveraging any comparative advantage in every possible state power domain. Bachmann and Putter write that 'every nation can be certain that their individual attempts at gaining competitive and military advantage is under threat from nations such the [Peoples Republic of China] who has discovered - long ago - that advantage does not have to be the fruit of entrepreneurial genius if it can be stolen' (Putter and Bachman, 2022). China's aggressive industrial espionage actions, which might legally be construed as criminal,[3] will increasingly marginalise and isolate the country from circles of innovation and knowledge -specifically with regards to dual-use technologies and sensitive military technology.[4] Chinese 'national security espionage' (Bateman, 2022, p. 65) campaigns suffer from disruption to networked espionage activities of Confucius Institute initiatives, for example.

[3] Complex arguments can be forwarded as to the criminal nature of industrial espionage based on the various Hague Agreements and Conventions attempting to regulate international IP rights, control, and ownership. 'The Hague Agreement, concluded in 1925, was revised at London in 1934 and at The Hague in 1960. It was completed by an Additional Act signed at Monaco in 1961 and by a Complementary Act signed at Stockholm in 1967, which was amended in 1979. As noted above, a further Act was adopted at Geneva in 1999.' (Summary of the Hague Agreement Concerning the International Registration of Industrial Designs, 1925).
That said, it should also be taken into consideration that China only ascended to the Hague Treaty in May 2022, which could be interpreted that China was under no legal obligation to avoid industrial espionage. (The Hague Notification No. 146 Hague Agreement Concerning the International Registration of Industrial Designs Geneva Act of the Hague Agreement Concerning the International Registration of Industrial Designs Accession by the People's Republic of China. (2022)).

[4] 'A partial "decoupling" of U.S. and Chinese technology ecosystems is well underway. Beijing plays an active role in this process, as do other governments and private actors around the world.' (Bateman, 2022).

Both Russia and China are known for their proclivity to steal SET intellectual property (IP): one recent endeavour from around June 2020 has been associated with the cyber-attacks on critical European healthcare infrastructure to steal COVID-19 vaccine-related IP being developed by Western companies such as BioNTech and Pfizer (Tessari & Muti, 2021, pp. 29-30). This is not only morally reprehensible against the backdrop of global suffering caused by the COVID-19 pandemic, but it also acts as a trigger to strengthen measures against espionage, which in itself reinforces their international isolation.

Another catalyst for isolation is interference in the political processes of sovereign countries and attacks on their critical infrastructure. The European Union regards Russia as a primary contributor to the proliferation of these acts (*Ibid.*). Global security consultancy firm Control Risks summarises this threat as being characterised by the Russian and Chinese espionage operations, demonstrated by the cyber-attack on the Norwegian parliament, amongst others, and industrial espionage 'targeting sectors and technologies of strategic importance to domestic industrial policies and economic development' (Control Risks Group Limited, 2020).

Strategic or great power Competition (Bachmann, *et al.*, 2020) between the United States and China and Russia also raises significant obstacles to keep Russia and China isolated. One aspect of such competition is associated with the resources in the Arctic as well as the Antarctic regions. Control Risks projects increased Sino-Russo intelligence activity resulting from this competition (Control Risks, 2020). Thus, foreseeing an increase of more aggressive espionage targets policy developments and technological niches in support of their geo-strategic (e.g., forward operating infrastructure such as those established by China at several locations around the globe) and commercial (oil, gas, minerals, and trade routes) ambitions (*Ibid.*).

Once a state has been classified as an (inter)national threat, doing business in a globally connected world, access to foreign investment and access to necessary networks are negatively impacted. The number of millionaires

(estimated at 15,000) who are expected to leave Russia as a result of the Russo-Ukraine war, the resulting international sanctions, and an overall tarnished Russian national brand (Neate, 2022) are all examples of the consequences of Russia being viewed as a pariah state. According to London-based investment and immigration firm Henley and Partners, which specialises in immigration of wealthy clients to Europe, approximately fifteen percent of all Russian millionaires (in USD) will have exited Russia by the end of 2022. While not totally new, economic sanctions came of age in the 20th century[5], gaining improved efficiency over the years. For example, and critically so for Russia's national credibility as a superpower, Russia is losing civilian contractors in certain areas within the armed forces due to compensation issues (Reich & Starr, 2022). Recently 'a Vladivostok shipyard was allegedly unable to meet 25 billion rubles' [*sic!*] worth of government orders to build two tankers, two missile boats, and to maintain and repair other vessels' (*Ibid.*), confirming some speculation on dependency of the Russian defence industry on Western technologies. As these sanctions[6] take effect, more Russian wealth will probably leave in the short to medium term. With funding and associated commercial networks vacating Russia (and China) in favour of more secure lodgings in, e.g., Malta, the UAE, or Mauritius (Neate, 2022), it disrupts the access of politicians, national industrial capabilities, and supply chains, as well as research and development linked to that funding and networks. This has an obvious disrupting effect on Russian armament production and certainly on any form of military technology innovation. It is projected that an increased emphasis will be made on espionage to overcome deficiencies in these areas as a state generated remedy.

[5] 'The first recorded use of sanctions was in 432 BC, when the Athenian Empire banned traders from Megara from its marketplaces, thereby strangling the rival city state's economy. It was not however until the 20th century that the use of economic sanctions became more prominent.' (Abughris, 2021).

[6] 'Fact Sheet: United States, G7 and Eu Impose Severe and Immediate Costs on Russia', (The White House, 2022).

Returning to the Cold War: the Russo-Ukraine War and Its Impact on Russian Espionage

The February 2022 Russian invasion of Ukraine not only exposed Russia's imperialistic tendencies but also uncovered some of the primary fault lines within Russian defence and security capabilities (Jones, 2022 and Ingalls, 2022). A visible fissure is the relatively dated Russian military technology that was on display during the first 100 days of the Russo-Ukraine War (Newman, 2022), resulting in the significant depletion of available combat capabilities (Sly, 2022) due to high rates of destruction and attrition achieved by a more agile Ukraine. Even modern and more advanced Russian military technologies fielded in the face of asymmetric defences (examples include 'high-end heavy-armor platforms, such as T-72B3s, T-90s, and T-80 variants – including the latest T-80BVMs' (Kasapoğlu, 2022), T90M and T-14 Armata tanks (WION, 2022), which hasn't been fielded yet) turned out to be inferior resulting in catastrophic operational failures (Kasapoğlu, 2022) and revealed a strategic Russian disadvantage.

Resulting from inadequate military (Jones, 2022) and defence industrial planning (Kasapoğlu, 2022) combined with executive arrogance (or lack of professionalism) (Jones, 2022) and low morale/discipline (Jong, 2022), Russia failed to capitalise on a critical advantage it had early in the campaign – i.e., mass. These issues are highlighted in a quote from 'The Russian Defense Industry: A Distressed Brand - Expecting a short war' (Kasapoğlu, 2022) in which Ukrainian forces quickly folded, the Russians made no effort to ramp up production before the invasion, and although they have presumably now done so, their defense industrial complex does not have the capacity to keep up with the very high rate at which Russia is expending artillery shells (Sly, 2022). These issues could have been mitigated with enhanced intelligence operations better analysing the adversary and own operational and defence industrial (Reich & Starr, 2022) capabilities to do supply-support. The backlash against Russian aggression became evident in the unexpected level of international solidarity (European Commission, 2022) against the invasion as well as in the subsequent wave of sanctions (European Council, 2022), which

isolated Russia from critical supply-chains, e.g., resulting in surface-to-air missile production capabilities shutting down due to the unavailability of imported components (Reich & Starr, 2022).

Another strategic miscalculation that will fuel future Russian espionage efforts resulted from the *en masse* expulsion of Russian diplomats internationally (The Economist, 2022) – significantly disrupting diplomatic leverage and espionage architecture. Such disruption is alluded to in the statement Sam Lichtenstein alludes to such disruption stating that '[a]mid the intense global media coverage of the military conflict in Ukraine, another battle is being waged largely in the shadows: Russia's spy network across Europe is being decimated' (Lichtenstein, 2022). The chief of MI6 recently stated that Russian espionage capabilities in Europe were halved after the expulsion of 'more than 400' intelligence officers across Europe with several 'deep-cover spies' and 'illegals' arrested or exposed (Bertrand & Sciutto, 2022 and BBC News, 2022). With Russia isolated – diplomatically, economically, and technologically – a special effort can be expected to gain access to knowledge with which to modernise and innovate.

Russia's intelligence agencies are belied to be on 'war-footing' as a result of the unfolding failures in the Russo-Ukrainian War,[7] which could be interpreted as ramping up aggressiveness and innovativeness. For example, Jamali and Soldatov project increased vigour in the Seattle region (Ingalls, 2022), considered the hub of US technology, military infrastructure (e.g., the Trident nuclear submarine base), and critical national industries such as Boeing (*Ibid.*).

Limiting Russian defence and security development and modernisation as a key NATO priority is called for by Franklin D. Kramer and Barry Pavel during 2022. They state that 'NATO, along with other relevant institutions, should help organize long-term limitations on trade with Russia that would achieve this effect' (Kramer & Pavel, 2022 and Kramer, 2022). The authors

[7] Andrei Soldatov 'is renowned for his inside reporting on Russia's three spy agencies and is a senior fellow with the Center for European Policy Analysis' (Ingalls, 2022).

recommend that NATO must collaborate and cooperate with the relevant organisations and states to make sure that trade in support of 'Russian military capabilities is prohibited' (*Ibid.*). This will certainly add to the renewed focus of Russian espionage operations in support of its national security objectives and countering international efforts to isolate the country. This echoes the comprehensive package of international sanctions and export controls currently in various stages of implementation, inclusive of dual-use material and knowledge and technology export control that are required for military capabilities.

Thus, with the expected levels of isolation expanding, Russia will probably travel with larger diplomatic groups to events where it is still allowed to attend in future. For example, Russia is a member the Wassenaar Arrangement (WA)[8] and usually attends with approximately four delegates. Russian attendance of the various WA meetings and programmes (*Ibid.*) will probably be maximised to unlock opportunity for new 'diplomatic' staff to officially enter Europe to meet existing and potential future assets as part of espionage networking.[9] This is but one opportunity available. Another example was the recent Russian attempt to activate a GRU agent within the International Criminal Court in The Hague, Netherland (Muniz, 2022), foiled by the Dutch General Intelligence and Security Service. This would have provided much needed information and possible access to other opportunities in the run up of future war crimes investigations (and even prosecutions) stemming from the Russo-Ukraine War(s) and the Russo-Georgia war (Muniz, 2022). However, because there is such a focus on Russian HUMINT operations, their focus will probably shift significantly towards other capabilities.

[8] See more, The Wassenaar Arrangement, 2022.

[9] The Wassenaar Arrangement has 42 members – Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Türkiye, Ukraine, United Kingdom, and United States (*Ibid*).

Cyber-espionage is being used increasingly by Russia. In 2018 a former GRU (Soviet Chief Intelligence Office) agent was caught for cyber-attacks on the Organization for the Prohibition of Chemical Weapons' Wi-Fi network (Deutsche Welle, 2022). This could have provided much needed cover for Russian chemical weapons programmes and usage in conflicts around the globe. Based on the disruption to the Russian HUMINT networks discussed *vide supra* and the difficulty it might face to re-establish and/or expand Russian HUMINT capabilities in Europe and the United States, Russia will probably revert increasingly to cyberespionage (Volz, 2022). Cyberattack incidents tracking data could be used in future to verify the trend vectors.

The Russian cyber-offensive against Ukraine (2022) did not deliver the advantage that Russia required and expected, neither regarding the pre-invasion battlefield preparation nor during the first 200 days of the invasion (Jones, 2022). Similarly, one year later, offensive Russian cyber capabilities have deteriorated even further. Although Ukraine was subjected to a significant number of cyber-attacks and electronic warfare operations, its military and society did not lose the ability to function coherently. The Russian intelligence services led cyber offensive utilised an assortment of techniques against Ukrainian critical infrastructure (40 percent of the attacks) and government (32 percent of the attacks) (Jones, 2022 and Microsoft, 2022). This was a targeted attempt to cripple Ukrainian political astuteness and fighting spirit and to conduct espionage on a mass scale in support of Russia's military objectives (Jones, 2022). Choosing a 'hybrid' counter approach in terms of actors and means involved, Ukraine responded asymmetrically by calling on the international hacker-community to support Ukraine in its defence against this expanded Russian cyber-attack campaign (Jones, 2022 and Alspach, 2022). 'The Russian military faced considerable operational challenges, in part because of outside state [amongst others – the US Cyber Command] and non-state [amongst others – Microsoft Threat Intelligence Center (Microsoft, 2022) and SpaceX/Starlink satellites (Ankel, 2022)] assistance to Ukraine to identify cyber and electronic warfare attacks, attribute

the perpetrators, and assist with remediation' (Jones, 2022). Thus, Russian attempts to exploit intelligence and counterintelligence measures to secure advantages were swiftly parried, paralysed and, in some cases, eclipsed. These setbacks inform our belief that Russian cyberespionage and attacks will relent, adapt, and expand (Volz, 2022) to compensate for loss in capabilities, reputation, and access to intelligence.

Russian military doctrine (Novosti, 2020) also supports the projection of continued emphasis on aggressive espionage operations – paralleling their quest for technology and other strategic intelligence that would support their national interest – but more recently, it acts as an impetus to recover from their strategic miscalculations in the Ukraine war.

A catch-22 situation seems to be in play. The overall inferior performance of the Russian cyberespionage capabilities and abilities during the current Russo-Ukraine War could result in greater emphasis being placed on Russian HUMINT. However, its HUMINT capability was significantly disrupted due to the *en masse* expulsion of Russian diplomats. This process started around 28 February 2022 and continued into April 2022. By 8 April 2022, four hundred (alleged) Russian intelligence personnel embedded within diplomatic and consular staffs have been expelled numerous countries (Westfall and Simon, 2022). These events provide significant motivation for refocussed Russian espionage efforts on more cyberespionage and re-establishing HUMINT networks. With a severely disrupted diplomatic footprint internationally, Russia will have to be innovative in their approaches outsmarting Western counterintelligence.

Veiled under the pretence of commercial enterprises and similar to the Chinese BRI, albeit at a smaller scale, is the Russian use of hybrid warfare tactics and techniques to purchase real-estate in foreign countries of interest. There is the interesting case of the Airiston Helmi real-estate company that wanted to purchase real estate located in the Finnish Archipelago (the Turku archipelago) (Yle News, 2018 and Normark, 2020). The estate featured advanced technological capabilities and forward-basing space – all within a

strategically Finnish sea transport route and 'key seabed communication cables' (*Ibid.*). This is probably but one example, which if successful, would have provided Russian security forces with critical capacity to conduct espionage within Scandinavia. The other asymmetric example of moving real-estate that were probably used to host espionage assets and facilitate such activities are the vast number of Russian oligarch-owned superyachts (Gregorian, 2022). The disruption of this vast network of mobile platforms for networking at all levels by international sanctions, with the ability to host HUMINT, IMINT and SIGINT capabilities and any of the Russian security service personnel (FSB, GRU, or SVR), leaves another gap in Russian espionage capabilities. Future expansion in this sector should be closely monitored as an indicator of the renewal of specific capabilities.

Russia will emerge from the current Russo-Ukraine war as a nation deeply engaged in introspection on how to survive international sanctions whilst systematically recovering depleted military *matériel* stock levels and re-evaluating technology requirements for the future and for the modernisation of what is still in stock. The loss of so many HUMINT assets in key technology-leading countries supports the projection that Russian espionage will not be any less aggressive but will probably increase to re-established broken networks and assets and to establish new assets and networks necessary to circumvent the effects of sanctions and the negative effect of the largescale expulsion of diplomats during 2022.

Vulnerabilities created by Western oil and gas embargoes coming into effect during 2022 might create opportunities for Russia to trade energy for information, technology, and access to new networks in support of espionage. The expectation would be that Russia will increase its cyberespionage considerably based on its 'stand-of' characteristics. Evidence of this became already available in June 2022 – 'Russian intelligence agencies have increased the pace of cyberattacks against nations that have provided aid to Ukraine, according to new research published Wednesday by Microsoft Corp' (Volz, 2022). Reuter reports the same – 'Russian government hackers have

conducted multiple cyber spy operations on countries allied with Ukraine […]'. In the past, Moscow has denied conducting foreign cyber espionage missions, saying it 'contradicts the principles of Russian foreign policy' (Siddiqui, 2022). Excessive increases in activity on platforms such as Twitter have already been detected. Other social media platforms will also fall victim to this trend of gathering social media intelligence (SOCMINT) (Putter & Henrico, 2022).

Drawing the Bamboo Curtain – Chinese Espionage

In July 2022, The Director of the US Federal Bureau of Investigation stated that China poses the most significant 'long-term threat to [US] information and [IP]' and economic prowess based on their aggressive 'counterintelligence and economic espionage' (FBI, 2020).[10] Similarly, the Director of US National Intelligence testified before the US House Intelligence Committee in March 2022, asserting that China represents an 'unparalleled priority for the intelligence community due to the fact that China is coming ever closer to being a peer competitor to the [US] economically, militarily and technologically' (Garamone, 2022). This testimony was reinforced by the joint FBI-MI5 statement of July 2022, stating that 'MI5 is now running seven times as many investigations related to activities of the Chinese Communist Party compared to 2018' (Corera, 2022). Then, on 22 July 2022, the Head of MI6 stated that the United Kingdom is currently (and into the future) allocating more resources to the threat posed by China to 'Western governments and societies […] than to any other single subject within the service, saying it had just moved past counterterrorism in terms of importance' (Bloomberg, 2022). This clearly shows the extent and threat of Chinese espionage efforts.

What makes China a dangerous opponent is their (autocratic) ability to bring the entire Chinese government to bear on national interest and security issues, a truly whole of government approach with Chinese characteristics. Amongst

[10] Also, in the latest joint statement by the heads of the FBI and MI5 - Gordon Corera (BBC News, 2022) and Bateman (2022).

several economic, defence, and security related expansionism initiatives (Kruger, 2021), e.g., the BRI, China's national ambition to reunify with Taiwan, and become a superpower (better yet, replace the United States as the world leader) – China presents the 'broadest, most active and persistent cyber espionage threat to U.S. government and private sector networks'.[11]

China targets every possible advantage of leading SET nations to access SET-related IP (Chinese industrial espionage) as well as military/security classified material, political action, and counterespionage (Chinese national security espionage) (Bateman, 2022, p. 65). Then, there is a shift to cyberespionage. Jon Bateman writes that this cyberespionage results in very successful 'bulk collection efforts', all enabled by 'remote cyber operations' which precludes the requirement for 'insider access to U.S. systems, companies, or supply chains' (Bateman, 2022, p. 65). This standoff capability will just expand and increase in effectiveness into the future but can probably be managed with technology and counterintelligence defences. However, what Loch Johnson (2010) labels 'old-fashioned espionage, known as human intelligence or "HUMINT"" (Johnson, 2010, p. 7), referring to the age-old use of people to acquire the information required by their governments, will remain a significantly more complex risk, and more so in the case of China, to mitigate for democratic and open societies like the West.

Chinese HUMINT is enabled by mass – the fact that the Chinese expatriate communities worldwide are numerous, growing and integrated into national societal structures and culture in several countries. For example, the US Marine Corps enlisted its first Chinese person as far back as 1944. In 2016 the US military had 52,433 'Asian Americans' on active duty (Centre for Minority Veterans, 2022). When considering the size of the US security services (CIA, FBI, Homeland Security, etc) and the unparalleled size of the US SET community – the numbers of Chinese and/or Chinese heritage people

[11] Quoting Avril Haines in Garamone, 2022.

vulnerable to Chinese subversion (or threats to their families back in China) is a significant vulnerability for Western national security.

This problem is no different in several other developed and developing countries worldwide – albeit with scale differences. In fact, the US Academy for Cultural Diplomacy (Academy for Cultural Diplomacy, 2022 and Goodkind, 2019, p. 23) estimates a Chinese diaspora of approximately 39.5 million persons in 130 countries worldwide. In Africa, South Africa has the largest Chinese diaspora amongst African countries – estimated at 500,000 in 2012 and growing (*Ibid.*). Australia, a key NATO partner state in the Indo-Pacific, has an estimated 749,000 people of the Chinese diaspora (*circa* 2011) (*Ibid.*); the United Kingdom follows with 630,000 (circa 2011) while France has 540,000 (*circa* 2011) Chinese nationals (*Ibid.*). These observations do not imply that every Chinese national is an automatic asset for hostile espionage, as the Chinese diaspora is not homogenous and often even anti-CCP. However, in the context of espionage activities and host state vulnerabilities, the question that has to be asked is how national security agencies will be able to cope with the potential for espionage activities given the size of these diaspora communities. This is further complicated by a duality to the vulnerability. The Chinese diaspora have integrated over an extended period into the societies of many countries and are now accepted as part of the background. On the other hand, and from a reciprocal point, it is nearly impossible for Western expatriates to integrate as a diaspora community in China, thus complicating the capability of Western HUMINT collection in China (other than cyberespionage).

These diaspora communities make it possible to export other instruments that can be employed by the Chinese national security apparatus as capabilities for subversion and espionage. This is complicated by the reality that probably all primary Chinese business enterprises internationally 'ha[ve] an internal "cell" answerable to the [Chinese Communist Party (CCP)] to drive the political agenda and ensure that the company is compliant with political directives' (Gardner, 2020). This CCP link has been enshrined in national Chinese law since 2017: under its National Intelligence Law of 2017, all Chinese companies

are required to assist, support and cooperate when requested by the government to provide intelligence (Bachmann & Anthony Paphiti, 2019). Another known state-sponsored enterprise is the Chinese Confucius Institute, established *circa* 2004 and successfully exported internationally – 'enrolling more than nine million students at 525 institutes in 146 countries and regions' (Edwards, 2021 and Tessari & Muti, 2021). The potential for subversion and espionage is part of 'a key stratagem of China's 'soft war' (*Ibid.*) or 'soft power' (Yle News, 2022) against those nations successfully penetrated. Such 'soft war' takes place below the threshold, as a non-kinetic warfighting approach that takes place in the 'grey zone' of kinetic and non-kinetic operations and is manifest in China's so called 'unrestricted warfare' under the subcategory of the 'three warfares' of influence operations that take place in the perceptual domain of information operations (Mosquera & Bachmann, 2020).

The Confucius Institutes are modelled after internationally recognised cultural institutes such as Alliance Française (France) and the Goethe Institute (Germany). However, they have been revealed as CCP-funded propaganda and espionage platforms (Edwards, 2021). The exposure of the corrosive effects of the Confucius Institute's dogma/activities to national interests drives international re-assessment of access to domestic societal structures such as universities. Under suspicion of being a part of the CCP intelligence community (*Ibid.*), the Chinese Central Guidance Commission on Building Spiritual Civilization chairperson (April 2007) – part of the 'Propaganda Department of the Central Committee' of the CCP – stated that the Confucius Institutes were an 'important part of the CCP's external propaganda structure' (Yang, 2022).

Finland, Denmark, and Sweden recently closed Confucius Institutes operating within their borders (Yle News, 2022). Helsinki University will, henceforth, appoint their own Chinese language tutors because, according to the university, there is an increasing demand for Chinese language proficiency. This trend fits well with the massive Chinese diaspora community internationally. Of course, better Chinese language literacy within individual

countries has its advantages for political, economic, and SET reasons. However, it is a double-edged sword. The better people understand each other and converse in the same language, the quicker foreigners integrate into another country and the easier it is to engage in espionage. So, China might consider inviting foreign nationals to China for language training in future under the pretext of some cultural diversity programme to ensure that integration of Chinese nationals abroad has a higher success rate – thus increasing the likelihood of establishing and maintaining ever expanding networks for espionage.

The closure of the Confucius Institutes also eliminates the requirement for Chinese-paid staff to be in those countries. For example, the Confucius Institute's deputy director (Helsinki University) was deemed 'unacademic' whilst enjoying a close relationship with the Chinese embassy (*Ibid.*). Primary Chinese targets are '[A]merican academia, with its cutting-edge technology, access to American thought leaders, and ability to shape future generations of American citizens [however,] China knows that Confucius Institutes have become politically toxic, and it has shifted its focus toward other means of engagement' (Peterson, 2021). This toxicity led to the closing of seventy-one Confucius Institutes in the United States *circa* March 2021 (*Ibid.*), with a significant disruption to established Chinese networks due to the exfiltration of Chinese staff. Realising that their strategy has become exposed, the Chinese government can be expected to replace it with another programme to sustain established and sensitive espionage networks and assets. China immediately set into motion a rebranding campaign – *circa* 2021, the Chinese government set in motion deception manoeuvres to change the program structure to evade US policy regulations. For example, 'On July 1, 2021, one day after its Confucius Institute closed, the College of William and Mary established the W&M-BNU Collaborative Partnership with Beijing Normal University, according to the school. The Chinese university was the American school's former Confucius Institute partner, providing the programs the Confucius Institute used to offer' (Yang, 2022). This is a direct response to an indication that continued access to conduct espionage and subversion is required. The

next section focusses on offensive cultural programmes to imperialism disguised as economic development.

A key catalyst for current and increased levels of Chinese espionage is the BRI, China's ambitious global infrastructure development project. Aiming to controlling geo-strategic locations internationally for a dual military/economic purpose best describes the BRI. Consequently, the BRI is increasingly being associated with Chinese espionage and subversion activities (Palma, 2018). The Chinese BRI is used to collect information to 'damp dissent' and to control the 'debate and ideas where that has specific security and diplomatic consequences' (*Ibid.*). Such data collection occurs from various points - including but probably not limited to 'ecommerce platforms, Confucius Institutes, telecoms networks, transportation companies, hotels, financial payment institutions and logistics companies' – which is then channelled to centralised analysis centres in China (Palma, 2018). With this initiative exposed for its various threats, China will have to innovate new approaches to compensate.

Open criticism towards the Chinese government and their policies also seems to be a trigger for increased espionage against such perpetrators. For example, Malaysia could be targeted by increasing Chinese cyber-espionage activities due to remarks by the Malaysian Prime Minister about BRI contracting. Examples of cyber-attack using non-state and state capabilities are not in short supply according to Palma (2018). There is also the targeting of Chinese dissidents in the United States and other countries in an attempt to silence dissent. According to a July 2022 report, by employing both HUMINT operatives and cyberespionage and related activities, '[t]hese programmes are believed to be part of a wider, growing and multi-faceted intelligence effort' in support of CCP autocracy (Debusmann, 2022). Increasingly, China interferes in US politics as well as those of other countries when their policies are perceived as adversarial to the Chinese national interests (Corera, 2022). Based on these trends, it is not unrealistic to project increasing levels of cyber-espionage and -attacks in the short to medium term.

Staying with cyber-espionage, China has a healthy and growing cell phone software application and video (software) games industry exploitable for the collection of untold volumes of data for analysis (Bateman, 2022, p. 69-70). This has also already been released by the West and countries such as India that responded by banning a number of these applications (*Ibid.*). Thus, several of the Chinese espionage programs/capabilities have already been exposed, and renewed and innovative measures can be expected from China as a result. With cyber-espionage continuously being countered by targeted countries, an increase in Chinese HUMINT can be expected as relationship building is at the heart of any espionage engagement and is filled with complexities that seek to bypass logical conclusions about interest and security.

The Prospects

In a world already accustomed to aggressive Russian and Chinese espionage activities, it can be expected that Russia (and associated non-state actors) will retaliate with an enhanced espionage campaign targeting those countries and organisations that provide military and technological assistance (for example Elon Musk's Starlink satellite internet constellation (Jones, 2022) to Ukraine and any NATO partner country. The sanction-induced access-to-the-latest-technology prohibition against Russia will unlock a momentous ambition to obtain the latest technology knowledge. Aggressive espionage remains the preferred option. With a greatly reduced Russian diplomatic staff (and thus HUMINT capacity), usage of mobile platforms such as the Russian oligarch superyacht fleet and other real estate world-wide (typical espionage capability staging areas) and reliance on cyberespionage can be projected to display new vigour in the short to medium term. The Microsoft Threat Intelligence Center reported that there is evidence of such trends unfolding (Hope, 2022). However, information networks and their associated crevasses can be secured. Thus, the medium to long term will probably be remembered for an increase in Russian HUMINT activity worldwide – albeit focussed on countries with significant SET capabilities and knowledge and on those countries that have

access to these and that are willing to share information with Russia for access to energy commodities.

China is no different. With the Chinese Confucius Institute systematically exposed as an incubator for latent espionage capabilities and subversion, reliance will increasingly shift in the short to medium term to cyber-espionage (Corera, 2022). It can also be expected that Western institutions that financially gained from hosting the Chinese Confucius Institute will, together with China, innovate to maintain such lucrative enterprises – to the detriment of their national security. Reports of such adaptation appeared in June 2022: 'many once-defunct Confucius Institutes have since reappeared in other forms' (Sharma, 2022). This shows a clear intention to maintain established networks for espionage and the important link these Institutes form within the Chinese intelligence enterprise. They are also maintained in support of more mainstream efforts such as cyber-espionage because of their HUMINT focus.

Then there is the corrosive impact of Chinese imperialism in the Pacific, Africa, and even Europe through its BRI. An increase in Chinese HUMINT could be expected in areas of interest to the BRI and related strategic geographic locations. Again, cyber-espionage could be exploited to prepare the battlefield, but it invariably takes people to connect with other people.

Conclusion

There are several indicators that point towards the isolation of Russia and China for several and varied reasons that is disruptive to their espionage capabilities. It is projected that such disruptions will provide renewed vigour to their intelligence collection efforts. In the short term, cyber-espionage will probably take the lead based on its standoff characteristics and the fact that Russian and Chinese HUMINT networks are continuously and systematically disrupted. However, in the medium to long term, cyber-espionage will be supplemented by HUMINT (even overtaken) in the event of the targeted countries are successful in securing their critical cyber infrastructure. The more

targeted countries report successes against cyber-espionage and other forms of electronic and cyberspace-related collection, the more the focus will shift towards HUMINT. Expanding diplomatic staffs, collaborative university programmes, and economic development initiatives are used to achieve expanded HUMINT footprints across entire regions. Their systematic exposure will initiate innovative and aggressive measures by Russia and China to reinvigorate lost espionage capacities. Such vigour will be fuelled by the need of Russia to modernise their military and space capabilities – a typical realist anxiety related to great power competition. Although the West's capability to severely restrict Russia's economic growth and cash flow is significant, there are always countries and organisations that would facilitate information flow for access to cheap energy – in a survivalist, defensive, and/or functionalist tradition. Economic sanctions came of age during the 20th century and with it came sanction busting. In the case of China, the West might be content on having cleaned house of undue cultural influence in the short term. However, the medium to long term will be littered with new CCP initiatives masquerading as diplomacy, development, assistance with lowering the language barriers between China and the rest of the world, or academic and cultural partnerships with eloquent names. With certainty, the international community will be confronted with increased and probably more aggressive Russian and Chinese espionage activity as they are systematically relegated to the margins of the international community.

Disclosure statement

The authors hereby declare that no competing financial interest exists for this manuscript.

Data availability statement

No new data were created or analysed in this study. Data sharing is not applicable to this article.

Bibliography

Abughris, Noura (2021) 'A Brief History of Economic Sanctions', *Carter-Ruck*, 30 November 2021 [Online]. Available at: https://www.carter-ruck.com/insight/a-brief-history-of-economic-sanctions/ (Accessed: 26 August 2022).

Academy for Cultural Diplomacy. (2022) 'Chinese Diaspora', Academy for Cultural Diplomacy [Online]. Available at: https://www.culturaldiplomacy.org/academy/index.php?chinese-diaspora (Accessed: 20 June 2022).

Alspach, Kyle. (2022) 'Going on Offense: Ukraine Forms an 'It Army,' Nvidia Hacks Back', *VentureBeat.com*, 26 February 2022. [Online]. Available at: https://venturebeat.com/2022/02/26/going-on-offense-ukraine-forms-an-it-army-nvidia-hacks-back/ (Accessed: 21 June 2022).

Ankel, Sophia. (2022) 'Ukrainian Soldier Says Elon Musk's Starlink Satellites "Changed the War in Ukraine's Favour"', *Businessinsider*, 28 April 2022. [Online] Available at: https://www.businessinsider.co.za/elon-musk-starlink-satellites-helping-ukraine-fight-soldier-2022-4?r=US&IR=T (Accessed: 21 June 2022).

Bachmann, Sascha-Dominik & Gunneriusson, Hakan. (2015) 'Hybrid Wars: The 21st Century New Threats to Global Peace and Security', 43 (1) *Scientia Militaria* 2015, pp 87 – 88. Available at: https://scientiamilitaria.journals.ac.za/pub/article/view/1110/ (Accessed: 10 February 2023).

Bachmann, Sascha-Dominik (Dov) & Lee, Doowan (2020) 'The Silent Erosion of Sovereignty: A Sino–Australian Example,' *Wild Blue Yonder*, 11 May 2020 [Online]. Available at: https://www.airuniversity.af.edu/Wild-Blue-Yonder/Article-Display/Article/2178205/the-silent-erosion-of-sovereignty-a-sinoaustralian-example (Accessed: 10 February 2023).

Bachmann, Sascha-Dominik (Dov), Lee, Doowan, and Dowse AO, Andrew. (2020) '#COVID Information Warfare and the Future of Great Power Competition', *The Fletcher Forum of World Affairs 2020*, 44:2.

Bachmann, Sascha-Dominik (Dov), and Paphiti, Anthony. (2019) 'Why Huawei security concerns cannot be removed from US-China relations', *The Conversation*, 10 May 2019, [Online]. Available at: https://gcp.theconversation.com/why-huawei-

security-concerns-cannot-be-removed-from-us-china-relations-116770 (Accessed: 9 February 2023).

Baker, Christopher D. (2003) 'Tolerance of International Espionage: A Functional Approach', American University International Law Review Vol. 19, No. 5 (2003), pp. 1091-1113.

Bateman, Jon (2022) *U.S.-China Technological 'Decoupling'*, Washington DC: Carnegie Endowment for International Peace, Available at: https://carnegieendowment.org/files/Bateman_US-China_Decoupling_final.pdf (Accessed: 20 June 2022).

BBC News. (2022) 'Russia About to Run out of Steam in Ukraine - MI6 Chief', BBC News, 21 July 2022 [Online]. Available at: https://www.bbc.com/news/world-europe-62259179 (Accessed: 25 August 2022).

Bertrand, Natasha, and Sciutto, Jim. (2022) 'Russia's Ukraine War Effort Running "out of Steam" as Putin's Ability to Spy in Europe Cut in Half, MI6 Chief Says', KTVZ, 21 July 2022 [Online]. Available at: https://ktvz.com/politics/cnn-us-politics/2022/07/21/russias-ukraine-war-effort-running-out-of-steam-as-putins-ability-to-spy-in-europe-cut-in-half-mi6-chief-says-2/ (Accessed: 25 August 2022).

Center for Minority Veterans. (2016) 'Asian American and Pacific Islander Fact Sheet', Department of Veterans Affairs. Center for Minority Veterans v.3/17/2016 [Online]. Available at: https://www.va.gov/centerforminorityveterans/docs/factSheetAanhpiOnePage.pdf (Accessed: 20 June 2022).

Coker, James. (2022) 'Chinese Cyber Espionage Groups Increasingly Targeting Russia', *Infosecurity Magazine*, 8 July 2022 [Online]. Available at: https://www.infosecurity-magazine.com/news/chinese-cyber-espionage-russia/ (Accessed: 25 August 2022).

Control Risks. (2020) 'Cyber Threats in 2020 and Beyond - Nordic Strategic Outlook', Copenhagen: Control Risks Group Limited [Online]. Available at: https://www.controlrisks.com/-/media/corporate/files/our-thinking/insights/cyber-threats-in-2020-and-beyond-nordic-strategic-outlook/nordics-cyber-threat-report.pdf (Accessed: 22 June 2022).

Corera, Gordon. (2022) 'China: MI5 and FBI Heads Warn of "Immense" Threat', BBC News, 7 July 2022 [Online]. Available at: https://www.bbc.com/news/world-asia-china-62064506 (Accessed: 24 August 2022).

CRF.org. (2022) 'Conflict in Ukraine | Global Conflict Tracker', Council on Foreign Relations, 12 May 2022 [Online]. Available at: https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine (Accessed: 25 August 2022).

de Jong, Belle. (2022) 'Putin Left in the Dark and "Low Morale" among Russian Soldiers, Western Intelligence Says', *The Brussels Times*, 31 March 2022 [Online]. Available at: https://www.brusselstimes.com/214262/putin-left-in-the-dark-and-low-morale-among-russian-soldiers-western-intelligence-says (Accessed: 29 June 2022).

Debusmann, Bernd. (2022) 'Americans in the Crosshairs of China's Spy Game', *BBC News*, Washington, 9 July 2022 [Online]. Available at: https://www.bbc.com/news/world-us-canada-62100402 (Accessed: 26 August 2022).

Deutsche Welle. (2022) 'Netherlands Agency Says It Foiled Russian Spy Attempt to Infiltrate ICC', *Deutsche Welle*, 16 June 2022 [Online]. Available at: https://www.dw.com/en/netherlands-agency-says-it-foiled-russian-spy-attempt-to-infiltrate-icc/a-62162178 (Accessed: 22 June 2022).

Edwards, Lee. (2021) 'Confucius Institutes: China's Trojan Horse', *The Heritage Foundation*, 27 May 2021 [Online]. Available at: https://www.heritage.org/homeland-security/commentary/confucius-institutes-chinas-trojan-horse (Accessed: 20 June 2022).

European Commission. (2022) 'EU Solidarity with Ukraine', European Commission, [Online]. Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/stronger-europe-world/eu-solidarity-ukraine_en (Accessed: 21 June 2022).

European Council. (2022) 'EU Sanctions against Russia Explained', European Council Consilium, 8 June 2022 [Online]. Available at: https://www.consilium.europa.eu/en/policies/sanctions/restrictive-measures-against-russia-over-ukraine/sanctions-against-russia-explained/ (Accessed: 21 June 2022).

Faligot, Roger. (2019) *Chinese Spies: From Chairman Mao to Xi Jinping*. Hurst & Company.

FBI. (2020) 'The China Threat', *FBI*, 10 July 2020 [Online]. Available at: https://www.fbi.gov/investigate/counterintelligence/the-china-threat (Accessed: 20 June 2022).

Garamone, Jim. (2022) 'U.S. Intel Officials Detail Threats from China, Russia', U.S. Department of Defense, 8 March 2022 [Online]. Available at: https://www.defense.gov/News/News-Stories/Article/Article/2960113/us-intel-officials-detail-threats-from-china-russia/ (Accessed: 20 June 2022).

Gardner, Frank. (2020) 'The Spying Game: China's Global Network', *BBC News*, 7 July 2020. Available at: https://www.bbc.com/news/uk-53329005 (Accessed: 24 August 2022).

Goodkind, Daniel. (2019) 'The Chinese Diaspora: Historical Legacies and Contemporary Trends', Demographic and Economic Studies Branch, International Programs Population Division, August 2019, p. 23 [Online]. Available at: https://www.census.gov/content/dam/Census/library/working-papers/2019/demo/Chinese_Diaspora.pdf (Accessed: 20 June 2022).

Gregorian, Dareh. (2022) 'Here Are the Superyachts Seized from Russian Oligarchs', NBC News, 5 May 2022 [Online]. Available at: https://www.nbcnews.com/politics/politics-news/are-superyachts-seized-russian-oligarchs-rcna20346 (Accessed: 29 June 2022).

Hope, Alicia. (2022) 'Russia Accelerated Cyber Espionage against Ukraine's Allies During the Invasion, Warned Microsoft,' CPO Magazine, 8 July 2022 [Online]. Available at: https://www.cpomagazine.com/cyber-security/russia-accelerated-cyber-espionage-against-ukraines-allies-during-the-invasion-warned-microsoft/ (Accessed: 26 June 2022).

Ingalls, Chris. (2022) 'Seattle Could Be Primed for Russian Spy Operations Amid Ukraine Conflict', King5.com, 19 May 2022 [Online]. Available at: https://www.king5.com/article/news/investigations/seattle-russian-spy-operations-ukraine/281-5504e5a2-5e78-4111-9b67-0c5739512038 (Accessed: 22 June 2022).

Johnson, Loch K. (2010) *The Oxford Handbook of National Security Intelligence.* Oxford: Oxford University Press, p. 7.

Jones, Seth G. (2022) 'Russia's Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare', Center for Strategic and International Studies, 1 June 2022 [Online]. Available at: https://www.csis.org/analysis/russias-ill-fated-invasion-ukraine-lessons-modern-warfare (Accessed: 22 June 2022).

Kasapoğlu, Can. (2022) 'The Russian Defense Industry: A Distressed Brand', *Hudson Institute Commentary*, 15 April 2022 [Online]. Available at: https://www.hudson.org/research/17754-the-russian-defense-industry-a-distressed-brand (Accessed: 29 June 2022).

Konstantopoulos, Ioannis L, (2012) 'Intelligence and IR Theory: The Cases of Covert Action and Economic Espionage', in **Aristidis Bitzenis & Vasileios A. Vlachos, (eds)**, *Proceedings, International Conference on International Business (ICIB), 17-19 May 2012*, Thessaloniki, Greece: International Relations and European Integration Laboratory, University of Macedonia. pp. 65-80.

Kramer, Franklin D. (2022) 'Free but Secure Trade: Priorities in Support of National Security', *Atlantic Council*, 9 June 2022 [Online]. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/report/free-but-secure-trade-priorities-in-support-of-national-security (Accessed: 20 June 2022).

Kramer, Franklin D. & Pavel, Barry. (2022) 'NATO Priorities: Initial Lessons from the Russia-Ukraine War', *Atlantic Council*, 14 June 2022 [Online]. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/nato-priorities-initial-lessons-from-the-russia-ukraine-war/ (Accessed: 20 June 2022).

Kruger, Gary. (2021) *Strategic Subversion: From Terrorists to Superpowers, How State and Non-State Actors Undermine One Another*, Bloomington, IN: AuthorHouse.

Lichtenstein, Sam. (2022) 'The Impact of the Ukraine War on Russian Espionage in Europe, Part I: Rane', RANE Stratfor, 15 April 2022 [Online]. Available at: https://worldview.stratfor.com/article/impact-ukraine-war-russian-espionage-europe-part-i (Accessed: 22 June 2022).

Marlow, Ian. (2022) 'UK Spy Chief Sees Russia's Military Running "out of Steam" Soon', *Bloomberg*, 21 July 2022 [Online]. Available at: https://www.bloomberg.com/news/articles/2022-07-21/uk-spy-chief-sees-russia-s-military-running-out-of-steam-soon (Accessed: 25 August 2022).

Microsoft. (2022) *Ukraine,* Redmond, Microsoft Special Report, WA: Digital Security Unit, 27 April 2022 [Online]. Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd (Accessed: 5 June 2022).

Mosquera, Munoz and Bachmann, Sascha Dov-Dominik (Dov). (2020) 'How China uses strategic preconditioning in the age of Great Power competition' The Fletcher Forum of World Affairs, 18 May 2020 [Online]. Available at: http://www.fletcherforum.org/home/2020/5/13/how-china-uses-strategic-preconditioning-in-the-age-of-great-power-competition (Accessed: 9 February 2023).

Muniz, Luanna (2022) 'Dutch Say They Stopped Russian Spy from Infiltrating International Criminal Court', *Politico*, 16 June 2022 [Online]. Available at:

https://www.politico.eu/article/netherlands-intelligence-prevented-russia-spy-from-targeting-international-criminal-court-the-hague/ (Accessed: 22 June 2022).

NATO. (2020) 'NATO 2030: United for a New Era Analysis and Recommendations of the Reflection Group', North Atlantic Treaty Organization, 25 November 2020, p. 10 [Online]. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf (Accessed: 12 December 2022).

Neate, Rupert (2022) 'More Than 15,000 Millionaires Expected to Leave Russia in 2022', *The Guardian*, 13 June 2022 [Online]. Available at: https://www.theguardian.com/world/2022/jun/13/more-than-15000-millionaires-expected-to-leave-russia-in-2022 (Accessed: 21 June 2022).

Newman, Rick. (2022) 'Why Russia's Military Is So Shabby', *Yahoo! Finance*, 1 April 2022 [Online]. Available at: https://finance.yahoo.com/news/why-russias-military-is-so-shabby-214049654.html (Accessed: 25 June 2022).

Normark, Magnus. (2020) 'Hybrid Coe Strategic Analysis 15: How States Use Non-State Actors. A Modus Operandi for Covert State Subversion and Malign Networks', Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats, 10 November 2020 [Online]. Available at: https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-15-how-states-use-non-state-actors-a-modus-operandi-for-covert-state-subversion-and-malign-networks/ (Accessed: 22 June 2022).

Palma, Stefania. (2018) 'China Accused of Using Belt and Road Initiative for Spying', *Financial Times*, 15 August 2018 [Online]. Available at: https://www.ft.com/content/d5ccb654-a02c-11e8-85da-eeb7a9ce36e4 (Accessed: 20 June 2022).

Pazzanese, Christina. (2019) 'Harvard Expert Says Russian Spying Is Nothing New - Only the Technology Is', *Harvard Gazette*, 20 February 2019 [Online]. Available at: https://news.harvard.edu/gazette/story/2019/02/harvard-expert-says-russian-spying-is-nothing-new-only-the-technology-is/ (Accessed: 26 August 2022).

Peterson, Rachelle. (2022) 'China's Confucius Institutes might be Closing, but they Succeeded', National Association of Scholars, 31 March 2021 [Online]. Available at: https://www.nas.org/blogs/article/chinas-confucius-institutes-might-be-closing-but-they-succeeded (Accessed: 20 June 2022).

Prochko, Veronika. (2018) 'The International Legal View of Espionage', *E-International Relations,* 2018 [Online]. Available at: https://www.e-

ir.info/2018/03/30/the-international-legal-view-of-espionage/ (Accessed: 18 July 2022).

Putter, Dries & Bachmann Sascha-Dominik. (2022) 'Scoping the future counterintelligence focus', *International Journal of Intelligence and Counterintelligence*. vol 36, issue 2 (2023).

Putter, Dries & Henrico, Susan. (2022) 'Social media intelligence: The national security-privacy nexus', *Scientia Militaria - South African Journal of Military Studies, 50(1),* pp. 19-44. https://doi.org/10.5787/50-1-1345.

Rathbone, John P. & Jones, Sam. (2022) 'Tip of the Iceberg: Rise in Russian Spying Activity Alarms European Capitals', *Financial Times*, 27 March 2022 [Online]. Available at: https://www.ft.com/content/bd74a542-3ce3-44de-a93a-36dc5929912b (Accessed: 25 August 2022).

Reich, Aaron, and Starr, Michael. (2022) 'Russia's Military-Industrial Complex: Low Salaries, Mass Layoffs', *The Jerusalem Post*, 7 May 2022 [Online]. Available at: https://www.jpost.com/business-and-innovation/banking-and-finance/article-706060 (Accessed: 25 June 2022).

Ria Novosti. (2020) 'Shoigu Spoke About the Tasks of the Information Operations Troops', РИА Новости [Ria Novosti], 3 March 2020 [Online]. Available at: https://ria.ru/20170222/1488617708.html (Accessed: 21 June 2022).

Richelson, Jeffery T. (1997) *A Century of Spies: Intelligence in the Twentieth Century*. Oxford University Press, [Online]. Available at: https://www.amazon.com/Russian-Espionage-History-Soviet-Spying/dp/1480131725 (Accessed: 25 August 2022).

Sharma, Yojana. (2022) 'Confucius Institutes Reappear under New Names – Report', University World News, 30 June 2022 [Online]. Available at: https://www.universityworldnews.com/post.php?story=20220630152610783. (Accessed: 15 August 2022).

Siddiqui, Zeba. (2022) 'Russian Cyber Spies Attack Ukraine's Allies, Microsoft Says', Thomson Reuters, 22 June 2022 [Online]. Available at: https://www.reuters.com/world/russian-hacking-groups-step-up-cyber-espionage-ukraine-allies-microsoft-says-2022-06-22/ (Accessed: 28 August 2022).

Sly, Liz. (2022) 'Russia Will Soon Exhaust Its Combat Capabilities, Western Assessments Predict', *The Washington Post*, 26 June 2022 [Online]. Available at: https://www.washingtonpost.com/world/2022/06/25/ukraine-russia-balance-of-forces/ (Accessed: 25 June 2022).

Starr, Barbara. (2022) 'Top US General Orders Comprehensive Review of US-China Military Interactions', CNN Pentagon Correspondent, 19 July 2022 [Online]. Available at: https://amp-cnn-com.cdn.ampproject.org/c/s/amp.cnn.com/cnn/2022/07/18/politics/milley-china-military-review/index.html (Accessed: 20 July 2022).

Tessari, Paola & Muti, Karolina. (2021) 'Strategic or Critical Infrastructures, a Way to Interfere in Europe: State of Play and Recommendations', European Parliament, INGE Committee, pp. 29-30 [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653637/EXPO_STU(2021)653637_EN.pdf (Accessed: 21 June 2022).

The Wassenaar Agreement. (2022) 'The Wassenaar Arrangement', Available at: https://www.wassenaar.org/about-us/ (Accessed: 21 June 2022).

The Economist. (2022) 'Russia's Army Is in a Woeful State', *The Economist Newspaper*, 30 April 2022 [Online]. Available at: https://www.economist.com/briefing/how-deep-does-the-rot-in-the-russian-army-go/21808989 (Accessed: 15 June 2022).

The Economist. (2022) 'Russian Spooks Are Being Kicked out of Europe En-masse', *The Economist*, 7 April 2022 [Online]. Available at: https://www.economist.com/europe/2022/04/07/russian-spooks-are-being-kicked-out-of-europe-en-masse (Accessed: 15 April 2022).

The Guardian. (2022) 'FBI and MI5 Leaders Give Unprecedented Joint Warning on Chinese Spying', *The Guardian*, 7 July 2022 [Online]. Available at: https://www.theguardian.com/world/2022/jul/06/fbi-mi5-china-spying-cyberattacks-business-economy (Accessed: 26 August 2022).

The White House. (2022) 'Fact Sheet: United States, G7 and Eu Impose Severe and Immediate Costs on Russia', The White House, 6 April 2022. Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/fact-sheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia/ (Accessed: 25 August 2022).

US Federal Bureau of Investigation. (2020) 'The China Threat', FBI, 10 July 2020 [Online]. Available at: https://www.fbi.gov/investigate/counterintelligence/the-china-threat (Accessed: 25 August 2022).

Volz, Dustin. (2022) 'Russia Increased Cyber Espionage against Countries Supporting Ukraine, Microsoft Says', *The Wall Street Journal*, 23 June 2022 [Online]. Available at: https://www.wsj.com/articles/russia-increased-cyber-espionage-

against-countries-supporting-ukraine-microsoft-says-11655910000 (Accessed: 29 June 2022).

Westfall, Sammy& Simon, Maite Fernández. (2022) 'Which countries have expelled Russian diplomats over Ukraine? The Washington Post, 30 March 2022 [Online]. Available at: https://www.washingtonpost.com/world/2022/03/30/diplomat-expulsion-russian-embassy-expel/ (Accessed: 20 August 2022)

WION News. (2022) 'Warzone Decoded: How Ukraine Has Fractured Russia's Feared T-90 Tank', WION, 8 May 2022 [Online]. Available at: https://www.wionews.com/photos/warzone-decoded-how-ukraine-has-fractured-russias-feared-t-90-tank-477346 (Accessed: 30 June 2022).

World Intellectual Property Organisation. (n.d.) 'Summary of the Hague Agreement Concerning the International Registration of Industrial Designs (1925)', World Intellectual Property Organisation [Online]. Available at: https://www.wipo.int/treaties/en/registration/hague/summary_hague.html (Accessed: 25 August 2022).

World Intellectual Property Organisation. (2022) 'The Hague Notification No. 146 Hague Agreement Concerning the International Registration of Industrial Designs Geneva Act of the Hague Agreement Concerning the International Registration of Industrial Designs Accession by the People's Republic of China', World Intellectual Property Organisation [Online]. Available at: https://www.wipo.int/treaties/en/notifications/hague/treaty_hague_146.html (Accessed: 25 August 2022).

Yang, Lin. (2022) 'Controversial Confucius Institutes Returning to U.S. Schools under New Name', VOA, 28 June 2022 [Online]. Available at: https://www.voanews.com/a/controversial-confucius-institutes-returning-to-u-s-schools-under-new-name/6635906.html (Accessed: 29 June 2022).

Yle News. (2018) 'Monday's Papers: A Closer Look at Airiston Helmi's Land Grab and Speeding Penalty Changes', *Yle News*, 24 September 2018 [Online]. Available at: https://yle.fi/news/3-10419525 (Accessed: 23 June 2022).

Yle News. (2022) 'Helsinki University Closes China-Funded Confucius Institute', *Yle News*, 18 June 2022 [Online]. Available at: https://yle.fi/news/3-12500430 (Accessed: 20 June 2022).