



## Scoping the Future Counterintelligence Focus

Dries Putter & Sascha-Dominik Dov Bachmann

**To cite this article:** Dries Putter & Sascha-Dominik Dov Bachmann (2023) Scoping the Future Counterintelligence Focus, International Journal of Intelligence and CounterIntelligence, 36:2, 358-385, DOI: [10.1080/08850607.2022.2091414](https://doi.org/10.1080/08850607.2022.2091414)

**To link to this article:** <https://doi.org/10.1080/08850607.2022.2091414>



Published online: 01 Aug 2022.



Submit your article to this journal [↗](#)



Article views: 2697



View related articles [↗](#)



View Crossmark data [↗](#)



Citing articles: 1 View citing articles [↗](#)




DRIES PUTTER AND SASCHA-DOMINIK  
DOV BACHMANN

## Scoping the Future Counterintelligence Focus

**Abstract:** A summary of counterintelligence threat chokepoints from the perspectives of the United States, Israel, the European Union, Nordic countries, and South Africa are presented. These chokepoints seem to stem from geopolitical competitiveness and manifest as espionage, subversion, terrorism, and covert action in any accessible domain possible. The discussion of threat focus areas has been chosen after consideration of the ontology of such threats, including new security challenges like hybrid threats, grey-zone influences, and some specific threats propagated by the COVID-19 pandemic. The discussion concludes with a brief view on counterintelligence threat enablers, accelerators, and effects. The aim is to provide a comparative view of existing counterintelligence threats, agendas, and threat responses to increase both awareness and resilience.

Counterintelligence has never been more relevant than today. Post–Cold War, this renewed relevancy has gained momentum since 11 September 2001<sup>1</sup> with current trajectories branching out into new dimensions of grey-zone strategic thought, Chinese expansionism, a reinvigorated Taliban regime on

*Dries Putter was a South African Naval Officer with 30 years of service. He is currently on the Faculty of Military Science at Stellenbosch University in South Africa. The author can be contacted at  [putter@sun.ac.za](mailto:putter@sun.ac.za).*

*Sascha-Dominik Dov Bachmann is a Professor in Law at the University of Canberra in Australia. He holds a PhD from the University of Johannesburg (South Africa) and is currently a Fellow of NATO SHAPE for the Asia Pacific focusing on hybrid threats and lawfare.*

the rise, Islamic State and other Islamist terror groups expanding globally, the ubiquitous nature of malign cyberactivity, pandemic-related disinformation activities, and expulsions of diplomats due to espionage activities. Extant counterintelligence capabilities internationally are at the center of removing the proverbial mirrors from the room to lay bare the undisputed facts. But on what should these counterintelligence capabilities focus?

Michelle K. van Cleave, a leading authority on counterintelligence, technology policy, and national security<sup>2</sup> provides some perspective on possible focus: “Now our nation is at war, engaged in a conflict different in kind and scope than any in our past. Because we are at war, the potential consequences of intelligence and other critical information compromises are more immediate, jeopardizing U.S. operations, deployed forces, and citizenry.”<sup>3</sup> She expresses concern about the international trajectories taken by nations in their quest for survival, progress, and domination. The twenty-first century is also characterized by an immense density of very capable intelligence services “organized, trained, equipped, and deployed” to secure national interests.<sup>4</sup> This national interest can be juxtaposed against what is projected by Patrick Bury and Michael Chertoff that the “... continuing evolution of terrorism will require counterterrorism intelligence to also adapt.”<sup>5</sup> All these issues of survival, domination, progress, intelligence failure, and proliferation of terrorism are topics of national interest and security. All these issues played out in the very recent developments in the post-U.S./Afghanistan presence. With the Taliban reestablishing itself as the government of the day in Afghanistan,<sup>6</sup> those states that were part of the international coalition forces that removed the Taliban from power in Afghanistan more than two decades ago and had a presence in Afghanistan for the same length of time will face the daunting prospect of renewed attempts by the most extremist elements in the Taliban regime to construct the demise of the infidels. Was this the trigger for renewed focus on terrorism from a counterintelligence perspective?

Michelle van Cleave uses a shield-and-sword metaphor to describe the defensive and offensive relevance of counterintelligence contributions to national security.<sup>7</sup> However, with international landscape changes due to political and socioeconomic flux the “sword” and the “shield” need to change shape, strength, and possibly application to retain relevance for counterintelligence challenges beyond the time horizon that are the products of the entrepreneurial integration of national interest, criminal, and/or extremist activities and intent. If the focus on terrorism has been renewed, the “sword and shield” approach will need to adapt to new counterintelligence threats. Which other threats are prominent currently and for the future within the context of counterintelligence? The following discussion aims, in general, at highlighting the relevant counterintelligence focus areas that could

necessitate a “sword and shield” redesign among those nations at the forefront of counterintelligence capability. The article will conclude with some contextual observations on the South African counterintelligence predicament.

## COUNTERINTELLIGENCE DEFINED AS A GAMECHANGER

On the back of the morphing nature of foreign intelligence services there is recognition for the tactical/operational utility of counterintelligence in the national security value chain. Strategic utility is now percolating from the mass of U.S.-based national security strategies and capabilities.<sup>8</sup> Van Cleave posits that counterintelligence directly impacts national security efforts by defending against hostile attempts at penetrating governmental capabilities and with offensive operations against such foreign intelligence capabilities. Indirectly, national counterintelligence capabilities also bolster “national policy formulation” momentum by facilitating enhanced transparency to the “plans, intentions, and capabilities of foreign powers.”<sup>9</sup> The recent releases of intelligence into the public domain prior to the Russian–Ukraine invasion by the United States and United Kingdom is an example of this.<sup>10</sup>

Thus, rising from obscurity as the intelligence stepchild, counterintelligence is currently fighting (and will more so in the future) for first-born privileges within the Intelligence Community by presenting a value proposition that is a gamechanger. This value proposition might be the crucial catalyst to counteract perceived “[p]olitical divergences within NATO [North Atlantic Treaty Organization] [that] are dangerous because they enable external actors, and in particular Russia and China, to exploit intra-Alliance differences and take advantage of individual Allies in ways that endanger their collective interests and security.”<sup>11</sup> The United States defined this gamechanger (i.e., the value associated with counterintelligence capability), as follows:

Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities. (Executive Order 12333, as amended, U.S. Intelligence Activities)<sup>12</sup>

This definition packs the various focus points where counterintelligence is poised to contribute to a perception of national security. Although definitions of counterintelligence vary widely, the U.S. definition provides utility for the purpose of this article—expressing concisely on what to expect from whom. Although not universally accepted, it is authoritative in the

sense that it is used to guide probably the largest and most capable counterintelligence capability in the world today.

## **CONTEXTUALIZING COUNTERINTELLIGENCE STRATEGIC CHOKE POINTS**

Intelligence operations are commonly used by less-than superpower nations to acquire or maintain advantage. This is presumed to be a “classic asymmetric strategy.”<sup>13</sup> It is the role of counterintelligence—both defensively and offensively—to counter such ambition of foreign intelligence services. Thus, nations typically embark on trend analysis and the construction of national strategies to inform national counterintelligence programs’ policy guidance and resources. The reality dictates that not all is visible for public scrutiny—which would be counterintelligence suicide. When published policy, strategies, and trend analysis are considered comparatively, counterintelligence choke points reveal themselves, providing foreknowledge glimpses into prevailing and emerging national security threats, their actors, enablers, and accelerators. Some of these issues will be explored from a Western perspective. Of course, it should be assumed that those organizations and nations perceived as threats have similar, converse, perspectives about the Western nations. Some of these choke points reveal themselves when counterintelligence threat ontology is discussion.

## **TRENDING COUNTERINTELLIGENCE THREAT ONTOLOGY**

The predictability of commencing with a U.S. counterintelligence perspective is almost perverse. However, the merit is locked in by the fact that the United States is the nation that publishes widely about its national security—almost fashionably propagandistic. There is food for thought in this trend alone. If a superpower feels threatened by certain threat actors (state and nonstate alike) and threats such as espionage, intelligence activities, sabotage, assassinations, terrorism, and others—then surely other superpower nations and nations further down on the scale of national power should not accommodate counterintelligence naivety when choosing their respective brand of “sword and shield.”

It is useful to take an audit ever so often of what is perceived as being the threat agent(s) or actor(s). The United States regards these as foreign intelligence entities<sup>14</sup> in the form of “nation-states, organisations and individuals” with malicious anti-U.S. national interest intent. These are then further unpacked in a footnote in the “National Counterintelligence Strategy of the United States of America 2020–2022” to include “a known or suspected foreign state or non-state organization or person. [...] It includes foreign intelligence services—defined as state intelligence services—and can

also pertain to international terrorists, transnational criminal organizations, foreign cyber actors, or foreign corporations or organizations.”<sup>15</sup> It seems to be very diverse in scope, but it is essentially people (individuals or groups) with malicious intent and actions against the national well-being (security if you will) of a nation. Nothing is a threat if there is not a human involved. Humans act in various domains as dictated by several and varied socioeconomic, demographic, political, religious, and other factors.

Gadi Eisenkot and Gabi Siboni authored the “Guidelines for Israel’s National Security Strategy”—a less-than-superpower perspective—classifying threats as conventional, nonconventional, subconventional, and cyberspace and information threats.<sup>16</sup> Naturally, not all these national security threats should be the concern of counterintelligence organizations. Yet the “shield” provided by counterintelligence will be present to provide operational security to offensive and defensive activities. The Israeli Security Agency, responsible for counterintelligence, still uses the conventional counterintelligence definition<sup>17</sup>—“the protection of State security and the order and institutions of the democratic regime against threats of terrorism, sabotage, subversion, espionage and disclosure of State secrets [or insider threats].”<sup>18</sup> This is very similar to that of the United States. These threat constructs can be grouped within the categorizations of conventional, nonconventional, subconventional, and cyberspace and information threats. This provides levels of analysis for threat identification, analysis, and mapping that are not commonly found in definitions of counterintelligence. Complex threats typically have a presence across all or several of these domains or spaces.

In the spirit of growing the counterintelligence threat ontology, other aspects that need considering are those relating to both grey-zone operations and hybrid threats. When considering grey-zone<sup>19</sup> offensive actions, Russia and the People’s Republic of China (PRC) share the ambition to destabilize the United States and its allies. Such threats remain a primary threat to their national security and interests. Echoing sentiments about the Russo–Sino threat expressed in a strategic threat analysis done by NATO,<sup>20</sup> Emily Harding states eloquently that “Russia presents one of the most serious intelligence threats to the United States,” typically employing influence operations to disrupt voter behavior and (executive) decisionmaking. Similarly, the PRC is identified as a major national security threat due to their “continue expanding its global intelligence footprint... . Beijing has been intensifying efforts to shape the political environment in the United States to promote its policy preferences, mold public discourse, pressure political figures whom Beijing believes oppose its interests, and muffle criticism of China.”<sup>21</sup> This threat spreads very visibly under the guise of developmental assistance to an increasing number of countries, thus affecting

an even greater number of countries indirectly if the current case of security cooperation between the Solomon Islands and the PRC is considered<sup>22</sup> and all the nations affected by the PRC Belt and Road Initiative.<sup>23</sup> This seems to be from the playbook of allied Western democracies and is not novel at all. The current scope of these activities, however, might be considered—unlike any experienced thus far—driven by a greedy perversion for political and economic power, and ubiquitously enabled by national cybercapabilities as part of national covert action machinery.

A European perspective from the European Centre of Excellence for Countering Hybrid Threats posits hybrid threats to be unconventional (note the categorization using Israel's National Security Strategy) in nature. A hybrid threat could be defined as “coordinated and synchronized actions conducted by an actor whose goal is to undermine or harm the target by influencing its decision-making at the local, regional, state or institutional level. As such, hybrid threats could be conducted by both state and non-state actors.”<sup>24</sup> This definition recognizes the state/nonstate categorization of threat actors as well as a primary threat—undermining decisionmaking at all levels of society, or better known as subversion. Subversion was and is used in the ongoing Russian–Ukraine war at all levels of analysis.<sup>25</sup> Hybrid operations unpacked include (but are probably not limited to) action that

exploits vulnerabilities of democracies and institutions, benefitting from ambiguity not only in terms of detection and attribution, but also because of the intrinsic difficulty in classifying a hybrid event due to the use of various measures—conventional and unconventional – in different areas (political, economic, cyber, military, civil) by the attacker.<sup>26</sup>

At this juncture it must be said that hybrid operations are not just those perpetrated against democracies. They are surely also employed by democracies to achieve national security and interest ends. Continuing with the views of Tessari and Muti on hybrid operations, “[They blur] the lines that traditionally serve to identify and label a threat as well as manage its consequences and response. A hybrid action will try to exploit democratic, legal, procedural or institutional gaps, vulnerabilities and uncertainties.”<sup>27</sup> NATO sums the nature of “hybridity” up as follows: “The employment of a comprehensive, coordinated strategy of military and/or non-military instruments of power (IoP) across the DIMEFIL (Diplomatic, Information, Military, Economic, Financial, Intelligence, and Legal) spectrum used in an overt and/or covert manner in either a linear or non-linear fashion.”<sup>28</sup> Hybrid operations could be used by any capable regime (democracy or not) to undermine other regimes. This again brings into view the perspective of Van Cleave (mentioned earlier) and the concerns about the international



trajectories taken by nations in their quest for survival, progress, and domination—all national security objectives of the twenty-first century.<sup>29</sup> So, in a nutshell, hybrid operations are very complex, multidimensional threats—they are essentially a threat-of-threats (in the spirit of terms such as “system-of-systems”) stemming from a constellation of capabilities with no predetermined logic. It cannot be said with certainty that this is a new phenomenon, though—but at least this kind of threat now has a label. That said, it can be assumed that the effects of hybrid operations will be spurious and disrupt conventional counterintelligence practice and should thus become part of the scope of counterintelligence threat perspectives.

The construction of such a threat stems from national security strategies, capabilities, intent, and the collective imagination of those involved. The United States and its allies certainly endeavored to “exploit [totalitarian], legal, procedural, or institutional gaps, vulnerabilities, and uncertainties” when they decided to depose of the Hussein regime and the Taliban. What makes these operations possibly more pronounced are the enablers that are currently available that drive their complexity and deniability to new shades of greyness.

Some recent (well-published) examples of hybrid operations are the interference by foreign entities in presidential elections in the United States and France. The normal covert action<sup>30</sup> toolbox is deployed in such instances (e.g., “... propaganda, deception, misinformation/disinformation and other non-conventional tactics”).<sup>31</sup> The novelty inherent in the current hybrid attacks is their migration to cyberspace—translating into speed, intensity, and scale gains—enabled by swift evolutionary technology development trajectories and expanded international connectivity.<sup>32</sup> This phenomenon has not been illustrated better in history than in the Russian–Ukraine war.<sup>33</sup> It is when you consider covert action theory by William Daugherty, John Prados, and Mark Lowenthal<sup>34</sup> that one must wonder if hybrid action is not just another (more acceptable) name for covert action—a construct that has accumulated considerable bad foreign policy optics over the years. Also mentioned within the purview of hybrid threats directed to critical infrastructure is cyber and industrial espionage as well as information theft. Dubious manipulation of the media (i.e., shaping the narrative), typically combined with misinformation pollution are perceived to have an indirect impact on critical infrastructure security because of the side effects stemming from (typically) mob/riotous behavior.<sup>35</sup>

Thus, hybrid threats consist of a constellation of counterintelligence techniques and can thus be considered a primary threat that will attract a significant counterintelligence response from those targeted. The pervasiveness of hybrid threats will increase as event horizons become reality due to the enabling quality and affordability of advanced technology and the



(yet to be achieved) governability of cyberspace and the spreading discontent among the poor, disenfranchised, and middle-class societal segments.

In summary, it can be said that there is a common understanding and that counterintelligence threats emanate from both state and nonstate actors in the form of conventional, nonconventional, subconventional, and cyberspace and information threats, each of which consists of constellations of various threat activities, such as espionage, subversion, assassinations, terrorism, and hybrid operations/covert action and that these are enabled in complex ways by technological evolution and cyberspace.

### COUNTERINTELLIGENCE THREAT AGENDAS

Internationally, each country has its own threat perception based on geopolitical, socioeconomic, and military requirements stemming from national interests. Such national security estimates take on many and varied formats and find their way into the public domain for many reasons. Once in the public domain these expressions of threat and perceptions of insecurity can be scrutinized, analyzed and contrasted to find commonality and diversion that would assist future planning and resource allocation and decisions about collaboration (for example). The narrative that follows is utilizing this approach by considering a number of perspectives from various geographic areas around the globe.

#### NATO

NATO's analysis of the strategic environment allows for expression on various perceived threat choke points and some of the primary threat actors. Throughout its report "NATO 2030: United for a New Era Analysis and Recommendations of the Reflection Group,"<sup>36</sup> both Russia and China are posited as primary threats to international security from various perspectives. The report states that "Russia is deploying a broader hybrid toolkit including offensive cyber, state-sanctioned assassinations, and poisonings."<sup>37</sup> This also links with the opinion that covert action has become mainstream within hybrid warfare.

The "NATO 2030" report very concisely provides a glimpse at the typical choke point examples of NATO's threat perception: the "enduring threat of terrorism, instability along NATO's southern periphery, a dramatically changing technological landscape, numerous, vexing non-state threats, and man-made as well as natural risks."<sup>38</sup> This reiterates the 2010 Capstone of Hybrid Threats when you consider the definition for hybrid threats used by this document: "Hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives," coupled to "Hybrid threats do,

however, now present a significant challenge for the [NATO] Alliance and its interests, whether encountered within national territory, in operational theatres or across non-physical domains.” Thus, hybrid threat actors “may be ready to choose from the full range of terrorist, criminal, conventional and irregular means and methods available to them.”<sup>39</sup> These are very broad categories or strategic choke points and certainly not a finite list. Many of these will find their way into or are echoes from other multilateral and national threat analyses. They are certainly driven by one of the primary security environment drivers: “the re-emergence of geopolitical competition.”<sup>40</sup> These strategic-level drivers produce several and varied operational-level threats that require a counterintelligence response.

### *The United States of America*

Shifting the discussion toward national counterintelligence threat agendas it seems logical to consider the U.S. threat list as baseline due to the vast resources and capabilities the United States deploys to detect and analyze these threats. U.S. counterintelligence threats pivot around “... traditional spying, economic espionage, and supply chain and cyber operations,” which are targeting critical U.S. (and alliance) infrastructure by collecting “sensitive information” and establishing entry into critical infrastructure, access to sensitive research, technologies, related industrial secrets and intellectual property.<sup>41</sup> These operations are aimed at gaining critical understanding about the U.S. intelligence playbook, and to “...influence U.S. policy, or disrupt U.S. systems and programs.”<sup>42</sup> So, nothing surprising from a counterintelligence theory perspective if Hank Prunckun<sup>43</sup> was consulted. It is still just the struggle between two or more parties to gain foreknowledge required for the construction of competitive, security, and military advantage.

The U.S. “National Counterintelligence Strategy 2020–2022”<sup>44</sup> takes note of the projected longevity of the strategy’s relevance, which might be an indicator of the velocity of change or just an expression of the preoccupation of the United States with a very near horizon (!) and places particular emphasis on the use of “cyber operations, media manipulation, covert operations, and political subversion.”<sup>45</sup> These threat activities are aimed at collapses in social cohesion, unravelling the democratic fabric and integrity of alliances. These are all well-known target areas within the national interest construct of Western nations. They also fit comfortably into the grey-zone/hybrid and covert action basket. The virtual ubiquitous access to advanced (cyberrelated) technologies is fast becoming a threat vector due to the continuous lowering of the risk threshold for adversaries to engage in antinational interest activities.<sup>46</sup> As developing countries leapfrog toward ever more advanced stages of technology development, not always governed by strict accompanying regulations, so do the threat actors within these

countries, creating geographic and cyberspaces that feed off the willingness and ambition of developed nations to distribute developmental enablers to create new and more lucrative markets. Alternatively, these are distributed in a quest to “democratize” and stabilize a particular country or region—only to backfire when administrations change, and stabilizing forces are withdrawn while abandoning advanced capabilities and system-level technologies for the hibernating threat actor’s benefit. Recent events in Afghanistan provide us (for the second time) with evidence of this kind of (anti)national security strategy. Consequently, the failed U.S.–Afghanistan endeavor will provide a multitude of future counterintelligence challenges (avoiding a pessimistic view that might have described them as catastrophes) as the pro-Taliban activists and fighters migrate from the AK47 to Huawei 5G as an indication of expanded levels of sophistication but also hinting at a future (emerging) cyberthreat element.

A metalevel list of counterintelligence threat trends from the United States has been structured based on at least the following trends: (1) an increase in the volume of perceived adversaries that are targeting the United States, (2) increasing adversarial capability sophistication, (3) methodical entrepreneurship, and (4) expanded scope of potential “targets and vulnerabilities.”<sup>47</sup> This is only natural if one considers the recent conflicts of the United States; that is, the war on terror(ist groups), the “Global War on Terrorism,”<sup>48</sup> and the technology and economic war against China.<sup>49</sup> As state and nonstate counterintelligence threat actors build competence and develop capabilities with which to attack the United States and its allies, the rest of the world should get prepared for their roles as the collateral damage periphery. The United States and its allies are developing considerable and sophisticated defenses to counter these threats, probably resulting in these threat actors shifting their focus to more vulnerable targets in less developed and defended geographies and spaces. The point is, what is relevant to the United States is relevant to the rest of the world—albeit with contextual and scope variations. Thus, the rest of the world will face both state- and nonstate-directed conventional, nonconventional, subconventional, and cyberspace and information threats, comprising constellations of various counterintelligence threat activities such as traditional and possibly more innovative forms of espionage, subversion, assassinations, and hybrid operations/covert action with vastly accelerated effects.

Moving away from abstraction toward contextualizing the counterintelligence threat, the head of the U.S. National Counterintelligence and Security Center remains resolute about the formidable and expanding counterintelligence threat posed by the PRC, based on espionage-related statistics. He elaborated on the intellectual property theft perpetrated by the PRC, quantifying the damage to be “... as much as \$400 billion annually in

economic loss—effectively costing U.S. households about \$4,000 a year, after taxes.”<sup>50</sup> Now, smaller nations might not be experiencing the scourge of Chinese espionage as protuberantly as the United States, but every nation can be certain that their individual attempts at gaining competitive and military advantage are under threat from nations such as the PRC who discovered long ago that advantage does not have to be the fruit of entrepreneurial genius if it can be stolen. Sun Tzu might have included this cunning of the PRC in his *Art of War* scribbles if he was alive today. It is also only natural that adversaries will accumulate capability if it is available off-the-shelf or left behind when covert action programs are terminated with poor execution; the recent abrupt ending to the U.S.–Afghanistan adventure is a case in point. In defense of the United States, it was probably a good idea to leave Afghanistan and its people to find their own peace because of the main event gaining momentum (i.e., the reunification of the PRC and Taiwan as an extension of a historic Mao Zedong vision).<sup>51</sup>

Thus, note should be taken of the expressions about the shifting focus of threat vectors. The shift is away from an overemphasis on perceived terrorist(s) threats and counterterrorism toward “near-peer competitors” fielding significant intelligence capabilities in conventional spaces but also increasingly in grey zones. The PRC is perceived to be at the center of these surging, multifaceted national security threats.<sup>52</sup> The United States (and probably its allies) is currently on the defensive, defending against “... multidomain competition” with “near-peers” seeking to undermine (and succeeding in undermining) U.S. influence and capabilities.<sup>53</sup> Thus, the ship is veering away from anti-terror operations toward a more complex adversary that is intent on changing the world order permanently to suit its domestic and cultural interests. This description fits the PRC perfectly, since it presents all these attributes, and it does not have allies—thus, any change ambitions are solely to establish a Chinese world order.

The shift in U.S. counterintelligence focus from what is perceived to be “... low-tech, low-resourced adversaries (e.g., the Islamic State, al-Qaeda, and their subsidiaries to state actors such as the PRC and Russia)”<sup>54</sup> requires distinct recognition that the new focus areas and adversaries are robustly enabled with sophisticated, stolen, and home-grown technology. In the case of the PRC, these technology pincers are extended into every corner of the world by a vast Chinese expatriate community.<sup>55</sup> No other nation (bar possibly India) can field such a counterintelligence network.

There seem to be growing affirmation and consensus by senior U.S. officials that the PRC is a consummate competitor/adversary concerning influence peddling and “undermining Western-based norms.”<sup>56</sup> A scalpel technique being employed by the PRC that is cutting into the heart of foreign cultures is through education. The PRC Confucius Institutes franchises,

promoted through diplomatic channels by the Hanban and the PRC Education Ministry, are the scalpel to which we refer. Since 2014, censorship and propaganda programs promoted by these institutes were exposed to such an extent that “several universities in the US and Europe [did] not renew their contracts (NATO StratCom CoE).”<sup>57</sup> These institutes are also associated with science and technology intellectual property theft.<sup>58</sup> This provides new focus to the phrase “know your enemy like yourself” but also adds an additional facet—change the enemy to be more like yourself. Subversion in education clothes.

### *Israel*

Stepping away from the United States toward the Middle East, Barnea<sup>59</sup> and Eisenkot and Siboni<sup>60</sup> discuss perceived internal threats to Israel. Israel is certainly not a near-peer to the United States, Russia or the PRC; however, it is at the center of a premiere battle for sovereignty and survival as a nation-state. They classify and comment on these perceived threats as (1) focusing on an erosion of solidarity among segments of the population, (2) damage to belief in the justness of the Zionist cause, and (3) weakening of the internal legitimacy of Israel’s actions. The rifts cover social (between rich and poor), identity (Ashkenazi vs. Mizrahi, secular vs. religious), and political (right vs. left) terrain, with associated differing visions and values. These problems are exacerbated by the negative impact on outlying areas (Galilee, Arava, Negev) owing to demographic processes and neglect. These are typically areas that could be exploited by state and nonstate actors through covert action programs. Threats are classified according to being conventional, nonconventional, subconventional, and information/cyberthreat categories. Within the conventional space “... state militaries or non-state organizations operating like state militaries”<sup>61</sup>—in particular cyberspace and information operations”<sup>62</sup>—are a primary concern. The nonconventional space is still perplexed by nuclear proliferation, while subconventional spaces are dominated by “guerrilla warfare and terrorism,”<sup>63</sup> as well as the “use of the subterranean space for military and terrorist activity” and “activity in cyberspace” and an “enemy’s influence-wielding efforts.”<sup>64</sup> The information/cyber<sup>65</sup> category needs no introduction. It is perceived to be inundated with threats hailing from “... enemy states and organizations, entail capabilities designed to disrupt the functioning of Israel’s vital systems, upset daily life, conduct espionage, and steal data [...] efforts to influence opinion and consciousness, damage the legitimacy of Israel’s use of force, harm the legal system, and encourage economic and academic boycotts.”<sup>66</sup>

A combination of these categories and their peculiarities can quite easily be classified as a hybrid threat. It must be recognized that the strategic alliance between Israel and the United States will result in mutually assured

counterintelligence threats spilling over from one region to another ensuring continued diplomacy complexity, conventional tension, and a strong innovative and developing defense industrial complex straddling the Atlantic Ocean.

### *European Union (EU)*

The EU was also perplexed by the (1) “threats of sabotage and espionage,” (2) “Control over Intellectual property security,” (3) and the “increasing torment of cyber-attacks.”<sup>67</sup> Thus, the EU is taking action by sanctioning organizations and individuals that are known for their involvement in cyberrelated attacks such as the 2015 hacking of the German Parliament.<sup>68</sup>

A contemporary international concern is the COVID-19 pandemic. The development of a vaccine holds tremendous advantage from a diplomatic, security, and economic perspective—already aptly labeled vaccine diplomacy.<sup>69</sup> The EU has already found possible evidence of Russian and PRC espionage activities targeting the European medical and pharmaceutical complex to obtain information about vaccine development by companies such as Pfizer and BioNTech.<sup>70</sup> Yes—mercantilist greed mixed with a healthy dose of survivalist instinct will result in much espionage opportunism and an equal measure of counterintelligence leak stopping and shoring.

The EU views both Russia and the PRC as primary cyberthreats. The Russians have been active in state-sponsored offensive cyberactivities since at least 2004 throughout Europe—with targets including critical centers of control, such as parliaments, electoral campaigns, critical infrastructure, and supply chains.<sup>71</sup> Indirectly, due to the EU’s global connectivity with, for example, the United States, it would have experienced similar negative effects. Thus, within the context of counterintelligence, the offensive use of cybercapabilities against the EU will constitute a counterintelligence threat to all allied (typically NATO) and other (non-NATO) strategic partners. Connectivity is not the threat; it is the abuse thereof that has negative consequences catapulting the encryption software industry into a national security monolith.

Malicious cyberactivities, such as phishing, denial of service attacks, malware, and other cyberoperations, illegally targeting information technology infrastructures and networks are distinctly linked to the PRC’s expanding undersea cable network and related international digital community services. The network is aptly labeled the “Digital Silk Road.”<sup>72</sup> It is not the entrepreneurial initiatives taken by the PRC in their own national interest that are problematic. Every nation around the globe does exactly the same in various economic sectors where capacity is lacking or where perceived advantage is lurking. Rather, it is the digital capabilities and access these networks provide to the PRC with which to orchestrate hybrid

attacks on every, or any, target. According to Rebecca Arcesati,<sup>73</sup> these networks will extend and provide accessibility and connectivity into the “Baltic, Mediterranean and Arctic seas.”<sup>74</sup> The Arctic is becoming a highly contested geopolitical space (discussed from a Scandinavian perspective later in the article). The PRC-Arctic strategic intent reinforces threat perceptions by the Nordic countries considering the PRC. “This is an aspect that the EU should monitor more closely, since Chinese military forces are working actively on undersea surveillance and monitoring capabilities, leveraging civilian-military integration in this field.”<sup>75</sup> Notably, this is one of the hiding places for the U.S. Boomers,<sup>76</sup> resulting in counterintelligence congestion with ample scope error.

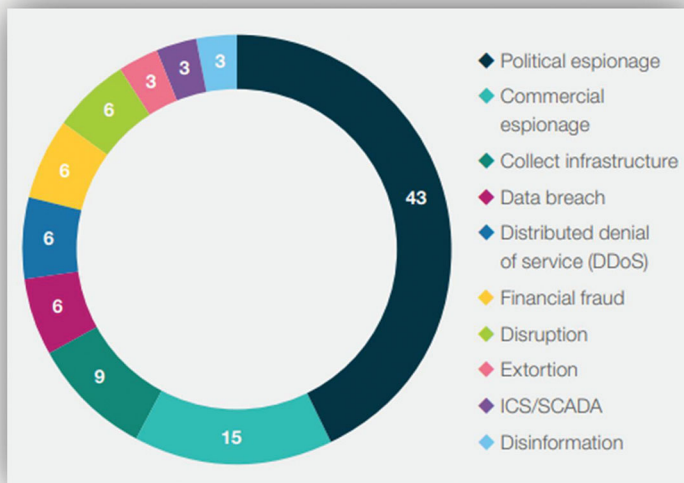
From a hybrid threat perspective the EU finds (1) “state-owned firms offering their services in key areas, such as highway construction, ports, and communications infrastructure”; and (2) “overdependence on Beijing in some critical services, supply chains or entities”—*typically the backbone of the “belt-and-road” and “silk road” strategic pincers*—of grave concern.<sup>77</sup> All of these infrastructures, entities, and supply chains are saturated with opportunities to subvert the populace and their democratic institutions, as well as expatriate export vehicles with which to sustain a global human intelligence (HUMINT) footprint. One wonders if these threats are recognized as only one part of a very complex puzzle being constructed by the Xi Jinping regime.

### *Nordic Countries*

Having touched on the contested Arctic circle, the Nordic countries<sup>78</sup> are also concerned about the cyberthreats emanating from the east. A recent example that reinforces this concern is the cyberattack on the Norwegian Parliament in August 2021. Then there is also preoccupation with commercial espionage activities that are targeting national strategic economic sectors and technologies as well as endeavoring to influence domestic industrial policies and economic development, “financial fraud and politically motivated disinformation and distributed denial of service attacks.”<sup>79</sup> Nothing new here. But what is not clearly stated relates to the swiftness and accuracy with which these attacks can now be delivered, which would be the spinoff effects of the ubiquitous access to advanced technology, software, and the persistent infectiousness of discontent among those that feel disenfranchised and psychotic leaders.

Control Risks labels these threats as Advanced Persistent Threat Groups (APTs). The primary identified APTs are expanding to countries such as Iran, Turkey, India, and North Korea.<sup>80</sup> The labeling of these threats is very apt and perfectly aligned with the trends from elsewhere in the world (i.e.,





**Figure 1.** Targeting intent of significant state-sponsored attacks in the Nordic region, 2018–2020 (%).

[technologically] advanced and tenacious). These are two of the fundamental takeaways for counterintelligence threat trends.

Nordic countries are mindful of their vulnerability to APT attacks during elections (Norway in 2021 and Sweden in 2022) and due to frictions between them and Russia and China. These typically covert actions will also be accelerated due to the U.S.–Russia–China geopolitical race for Arctic dominance. An important strategic effect of these issues is the decision by both Sweden and Finland to join NATO<sup>81</sup>—and thus breaking with a long history of neutrality. Control Risks is of the opinion that these dynamics will create an intelligence (and thus a counterintelligence) hotspot in and around Scandinavia. “The centrality of several Nordic countries in Arctic affairs and their high level of expertise in Arctic operations, including in the oil and gas and maritime sectors, likely make them attractive targets for espionage operations seeking to gain insight on Arctic policy positions, as well as technological solutions.”<sup>82</sup> Figure 1 shows that the perceived threat actions targeting Nordic countries are all typical counterintelligence threats.<sup>83</sup>

Cyberthreat actors will be targeting “government and public sector bodies, defence and national security agencies,” but more specifically focusing on critical infrastructure, capabilities, and knowledge—typically within the “oil and gas and energy [the renewable energy subsectors are of particular interest] sectors, finance and telecommunications economic sectors.” Private

contractors within the sectors are also considered targets, typically by state-sponsored Russian activities.<sup>84</sup> These threats will migrate to those countries that are achieving innovative breakthroughs in the renewable energy subsector—without robust counterintelligence measures in place, the redistribution of such innovation will take place swiftly, denying first mover commercial advantages and associated financial benefits to the trailblazers.

### *South African Counterintelligence Focus*

When shifting the focus from the developed world to a developing country such as South Africa it would not be any surprise to find vast differences from what has already been discussed. The South African National Strategic Intelligence Act 39 of 1994 defines counterintelligence as “... measures and activities conducted, instituted or taken to impede and to neutralise the effectiveness of foreign or hostile intelligence operations, to protect classified intelligence and to counter subversion, sabotage and terrorism aimed at, or against personnel, strategic installations or resources of the Republic.”<sup>85</sup> This closely resembles the U.S. definition. Considering the resources and capabilities that are being directed by the U.S. government counterintelligence definition, the parity inherent in the South African counterintelligence definition provides adequate direction to manage South African counterintelligence resources and capabilities. However, within the developmental state context South Africa only has a fraction (a bit of an understatement) of the resources and capabilities available to the United States and its allies. Considering the counterintelligence choke points discussed in this article alone, South Africa is wandering around in a room filled with “mirrors” created by internal adversarial competition,<sup>86</sup> with little focus on the new “mirrors” (or threats) being added to the wilderness each day.

In addition, South Africa cannot possibly allocate the vast resources that the developed Western countries are committing within the context of counterintelligence threat elimination and mitigation. That said, South Africa can ill afford the luxury of naivety about the counterintelligence threats directed at its democratic values, people, institutions, and infrastructure. Considering the full cup of percolated threats elaborated on above, South Africa will have to prioritize its counterintelligence prevention, preparation, response, and recovery according to national interests and available resources. Such a discussion always introduces the nexus between development and security. However, South Africa can ill afford undersecuring its vital interests in favor of developmental objectives and then find that those interests are compromised or pillaged and can no longer contribute to the developmental objectives.

## STANDALONE INTERNATIONAL COUNTERINTELLIGENCE CHALLENGES

COVID-19 is currently at the cliché level internationally. Nothing gets conceptualized or articulated without referring to its COVID-19 linkages. Counterintelligence is but another victim of this trend. That said, counterintelligence has real and significant linkages to the COVID-19 pandemic—and will probably generate similar linkages within the context of any future pandemic. The EU expressed deep concern about the counterintelligence fallout linked to the COVID-19 pandemic. These linkages are mostly within the context of critical infrastructure security—and specifically within the health and medical domains.

Layered on top of the very complex shifts within the health care fraternity to cope with different streams of health care issues that now must be separated from those related to COVID-19 is the vast opportunities stemming from the counterintelligence vulnerability of the medical fraternity culture, infrastructure, and other elements. Tessari and Muti place particular emphasis on the opportunities for cyberattacks camouflaged as COVID-19 emergency and/or management requirements. As such, cyberattacks target medical infrastructure and personnel with lures to download “... malicious apps, opening phishing emails covered up as official outbreak updates but, in reality, distributing malwares via attachments or links, or even add spywares or malwares in publicly available COVID-19-related maps and websites.”<sup>87</sup> The attacks are indiscriminate in the targeting—mainly due to the almost ubiquitous vulnerability to these types of attacks within the supply chain. “This has been particularly dangerous with respect to medical academic institutions involved in the development of vaccines or innovative treatments, as cyber criminals and state-sponsored espionage have posed risks in terms of accessing information to exploit commercial opportunities.”<sup>88</sup>

The pandemic also opened the eyes of (at least) the EU on matters of the negative consequences of international “interconnectedness.” This new awareness (of an old vulnerability) triggers questions about the level of reliance “on foreign technology, solutions and services, and what this means for our national-level resilience and vulnerabilities.” Although the world has benefited until recently from the technologies that make borders irrelevant, such benefits could turn out to be only a small constellation to the future costs associated with winning back that perception of being secure from the predatory intelligence and counterintelligence activities driven by the greed inherent in great powers competition.

### *Counterintelligence Threat Enablers and Accelerators*

Related to the continuously increasing sophistication of the adversaries—whether these counterintelligence threat actors are outsiders or insiders<sup>89</sup>—the

adversarial cyberactivity of nation-states should not be underestimated, primarily due to friction in the geopolitical space among the main actors, such as North Korea, the United States, the PRC, the United Kingdom, Germany, Israel, and probably others. This phenomenon highlights the fact that cyberenabled espionage and subversion activities are mutating in complexity and propelled by<sup>90</sup> integrated “... diplomatic, military and geopolitical developments.”<sup>91</sup> Geopolitics are a significant propelling agent for an “... increasingly fragmented cyber espionage threat.”<sup>92</sup>

The evolution and proliferation of new and evermore advanced smart technology as well as the miniaturizing of components, systems, and platforms are the multiplying force behind the current evolution of counterintelligence threats. “Emerging technologies such as artificial intelligence, quantum computing, nanotechnology, advanced materials, improved encryption, robotics, and the Internet of Things” fall within the ambit of threat accelerators. From a cyberenabled threat perspective, [Table 1](#) was compiled recently by the European Union Agency for Network and Information Security.<sup>93</sup>

A key takeaway from [Table 1](#) is the number of cyberenablers available to actual and potential counterintelligence threat actors. Not to be missed is that organized crime, nation-states, and big business have access to and deploy the full spectrum of enablers. When considering the permutations and possible combinations of actors and enablers, it is not difficult to construe cyberenabled counterintelligence threats (whether in standalone mode or hybrid combinations) as the most complex and ubiquitous counterintelligence threat known to humankind, which will probably take on quantum dimensions in the short to medium term. When this is combined with the threat perceptions outline (outlined earlier in the article) about the PRC—the current and future counterintelligence threat seems to be morphing into a (inter)national security threat with sophistication, mass (footprint), and tenacity under the current PRC regime, not yet encountered by humankind. While the West seems to be waking up to this predicament, there are a host of countries, particularly in the Global South (the “developing” world), that are being infiltrated by the PRC under the guise of economic development initiatives such as the “belt and road programmes.”<sup>94</sup> Several of these examples can be found in Africa, such as Djibouti.<sup>95</sup>

Paul Nantulya writes,

The end state of One Belt One Road is the building of a “Community of Common Destiny for Mankind” (人类命运共同体), defined as a new global system of alternative economic, political, and security “interdependencies” with China at the center (zhongguo, 中国). For this reason, Chinese leaders describe One Belt One Road as a national

Table 1. Cyberenabled Counterintelligence Threats

	Threat Agents						
	Cybercriminals	Insiders	Nation-states	Corporations	Hacktists	Cyberterrorists	Script kiddies
Malware	✓	✓	✓	✓	✓	✓	✓
Web-based attacks	✓		✓	✓	✓	✓	✓
Web application attacks	✓		✓	✓	✓	✓	✓
Denial of Service	✓		✓	✓	✓	✓	✓
Botnets	✓		✓	✓	✓	✓	✓
Phishing	✓	✓	✓	✓	✓		✓
Spam	✓	✓	✓	✓			
Ransomware	✓	✓	✓	✓			✓
Insider threat	✓		✓	✓		✓	
Physical manipulation/damage/theft/loss	✓	✓	✓	✓	✓	✓	✓
Exploit kits	✓		✓	✓			
Data breaches	✓	✓	✓	✓	✓	✓	✓
Identity theft	✓	✓	✓	✓	✓	✓	✓
Information leakage	✓	✓	✓	✓	✓	✓	✓
Cyber espionage		✓	✓	✓			

strategy (zhanlüe, 战略), with economic, political, diplomatic, and military elements (综合国力), not a mere series of initiatives.<sup>96</sup>

Thus, One Belt One Road constitutes a hydra. The strategic intent of the One Belt One Road initiative is being rolled out internationally, considerably complicating the counterintelligence landscape. Each project does not consist of just hardware (tar and mortar) but, more importantly, is accompanied by cyberelements (see, e.g., Huawei) as well as expatriate work forces arriving (and staying). It is a layered network of passive and active human and cyber networks.

A primary counterintelligence threat enabler is the Internet of Things (IoT). The “IoT brings the power of the internet, data processing and analytics to the real world of physical objects.”<sup>97</sup> Thus, the traditional counterintelligence enabler (e.g., sensors), can now be networked with several layers of nontraditional counterintelligence threat enablers, such as smart televisions, fridges, and so on. Oracle (n.d.) describe this phenomenon as

... the network of physical objects—‘things’—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools. With more than 7 billion connected IoT devices today, experts are expecting this number to grow to 10 billion by 2020 and 22 billion by 2025. Oracle has a network of device partners.

IoT is also widely used in industry—referred to as the Industrial IoT (IIoT): “... the application of IoT technology in industrial settings, especially with respect to instrumentation and control of sensors and devices that engage cloud technologies.”<sup>98</sup> The exponential growth that these networks enable in connectivity, in other words the exponential reduction in time and space requirements for counterintelligence activities, is at the leading edge of counterintelligence threat capability. The phenomenon is further enabled by cloud computing and artificial intelligence (AI),<sup>99</sup> which could provide the counterintelligence threat with the ability to develop its own permutation of singularity. “AI singularity refers to an event where the AIs in our lives either become self-aware or reach an ability for continuous improvement so powerful that it will evolve beyond our control.”<sup>100</sup> Once this evolution has taken place and matured a whole new set of mirrors is added to the “wilderness”<sup>101</sup>—and for that matter every possible space available to those involved in deception and denial.

The IIoT (also referred to as Industry 4.0.) is the enabler for “... smart manufacturing, connected assets and preventive and predictive maintenance, [...] power grids” [human settlements, supply chains, and logistics]. It is all very impressive if speed, adaptability, and flexibility are considered. What is

not said by Oracle<sup>102</sup> is the vulnerability of everything related to this “smartness” to adversarial counterintelligence activity.

Another enabler that is supposed to provide security (a deterrence from Prunckun’s perspective) is blockchain technology. This security technology is described as being “... essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain.”<sup>103</sup> Again, formidable redundancies and security; however, the fact that it is distributed translates that each individual ledger holder must always field similar counterintelligence deterrence characteristics and capabilities. This would be possible if controlled by singularity AI. However, once humans become involved, vulnerability enters the equation. Thus, incredible counterintelligence potential is still inherent in robust HUMINT operations.

### *The Effect*

It is important to acknowledge the effects of projected counterintelligence threats. Such acknowledgement is the first step towards effective responses. Hank Prunckun is of the opinion that effective responses are part and parcel of the counterintelligence process that aims at planning for prevention, preparation, response, and recovery in order to mitigate risk and vulnerability and eliminate threat.<sup>104</sup> Without such planning, resource allocation could end up skewed. The U.S. projects that the immediate effects stemming from successful adversarial attacks could cripple or destroy critical national infrastructure with obvious immediate to long-term military operational vulnerabilities that will result in diminished national strategic advantage across all physical and cyberdomains. Attacks against U.S. knowledge bases are postulated to have the same effect as critical infrastructure.<sup>105</sup> However, lost knowledge-based advantage will have a much longer negative effect on military and economic advantage. This phenomenon is true for all countries. The knowledge-hoarding practices of the PRC, for example, are thus an (inter)national security threat as they aim at positioning the PRC at the center of technological, economic, and military advantage. This is obviously a national strategic concern for Western democracies. Knowledge domination by countries such as the PRC has the potential to (re)shape the world order.

## **CONCLUSION**

Counterintelligence threats emanate from both state and nonstate actors in the form of conventional, nonconventional, subconventional, and cyberspace and information threats, each of which consists of constellations of various threat activities, such as espionage, subversion, assassinations, terrorism, and



hybrid operations/covert action and that these are enabled in complex ways by technological evolution and cyberspace. This article aimed to provide a counterintelligence threat focus analysis based on the threat perceptions by the United States, Israel, EU, Nordic countries, and South Africa. Although there does not seem to be any novelty to the threats in terms of the said activities that require novel counterintelligence responses, new technological developments mean that these traditional threats are now much better enabled to provide real-time effects and, in some cases, might be approaching singularity. These threats are also not the sole domain of the counterintelligence operative but have migrated to any individual actor who is motivated and capable to disrupt, create change, or get rich. Threat actors operate increasingly in spaces that are grey with capabilities that are stacked with hybrid integration. They seek to know the enemy like themselves but are also motivated to change the adversary into something familiar. Niche technology could be the answer to some of the denial-related complexity but could evolve into enablers that are no longer subservient to the human interface. South Africa subscribes to a comprehensive definition of counterintelligence. Considering South Africa being a developed country and within available and restricted resources, one will find it difficult to match the evolving sophistication of these threats and threat actors without a dedicated and robust effort by the state to invest in national counterintelligence capabilities. Alternatively, South Africa might have to consider a revision of what it considers counterintelligence to ensure parity between policy direction and available resources. To avoid a downgrading of the South African counterintelligence threat perception, serious consideration should be afforded to participate in international collaboration to unlock more resources and to ensure integrated responses to hybrid threats in grey zones under the guise of developmental initiatives.

## REFERENCES

- <sup>1</sup> Avner Barnea, "Counterintelligence: Stepson of the Intelligence Discipline," *Israel Affairs*, Vol. 23, No. 4 (2017), pp. 719–726.
- <sup>2</sup> A short biography of Ms. Michelle Van Cleaver, former national counterintelligence executive, is available at [https://www.uscc.gov/sites/default/files/Panel%20II\\_Van%20Cleave\\_Bio.pdf](https://www.uscc.gov/sites/default/files/Panel%20II_Van%20Cleave_Bio.pdf) (accessed 13 April 2022).
- <sup>3</sup> Michelle K. van Cleave, "Counterintelligence and National Security," School for National Security Executive Education (Washington, DC: National Defense University Press, 2007), p. 4.
- <sup>4</sup> *Ibid.*
- <sup>5</sup> Patrick Bury and Michael Chertoff, "New Intelligence Strategies for a New Decade," *The RUSI Journal*, Vol. 165, No. 4 (2020), p. 42.

- <sup>6</sup> Felicia Bolton, “Taliban Sweep into Afghan Capital after Government Collapse,” *News Nation*, 14 August 2021, <https://www.newsnationnow.com/world/taliban-seize-jalalabad-cut-off-afghan-capital-from-east/> (accessed 5 January 2022).
- <sup>7</sup> van Cleave, “Counterintelligence and National Security.”
- <sup>8</sup> *Ibid.*
- <sup>9</sup> *Ibid.*, p. 3.
- <sup>10</sup> Business Standard, “Secret Intelligence has Unusually Public Role in Ukraine War,” *Business Standard*, 3 April 2022, [https://www.business-standard.com/article/international/secret-intelligence-has-unusually-public-role-in-ukraine-war-122040300289\\_1.html](https://www.business-standard.com/article/international/secret-intelligence-has-unusually-public-role-in-ukraine-war-122040300289_1.html) (accessed 21 April 2022).
- <sup>11</sup> NATO, “NATO 2030: United for a New Era Analysis and Recommendations of the Reflection Group,” NATO Secretary General, 25 November 2020, p. 9, [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf) (accessed 13 April 2022).
- <sup>12</sup> United States, “National Counterintelligence Strategy of the United States of America 2020–2022,” Office of the Director of National Intelligence, 7 January 2020, [https://www.dni.gov/files/NCSC/documents/features/20200205-National\\_CI\\_Strategy\\_2020\\_2022.pdf](https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf) (accessed 18 August 2021).
- <sup>13</sup> van Cleave, “Counterintelligence and National Security,” p. 4.
- <sup>14</sup> The term “foreign intelligence entity” refers to a known or suspected foreign state or nonstate organization or person that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. It includes foreign intelligence services—defined as state intelligence services—and can also pertain to international terrorists, transnational criminal organizations, foreign cyberactors, or foreign corporations or organizations. 2018 National Threat Identification and Prioritization Assessment—United States, “National Counterintelligence Strategy of the United States of America 2020–2022,” p. 2.
- <sup>15</sup> United States, “National Counterintelligence Strategy of the United States of America 2020–2022,” p. 2.
- <sup>16</sup> Gadi Eisenkot and Gabi Siboni, *Guidelines for Israel’s National Security Strategy*, Washington Institute for Near East Policy (2019), p. 20, <https://www.washingtoninstitute.org/media/4613> (accessed 19 August 2021).
- <sup>17</sup> “... the ‘classic’ roles of counterintelligence organizations such as counterterrorism, counter-subversion, and counter-espionage.” Avner Barnea, “Integrating the Counterintelligence Discipline into Israel’s Security Concept,” *Strategic Assessment*, Vol. 23, No. 2 (2020), pp. 23–39.
- <sup>18</sup> Barnea, “Integrating the Counterintelligence Discipline into Israel’s Security Concept,” p. 24.
- <sup>19</sup> The U.S. Special Operations Command defines grey-zone challenges as “competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality.” In the words of Gen. Joseph Votel et al., “The Grey Zone is characterized by intense political, economic, informational, and military competition more fervent in nature than normal steady-state diplomacy, yet short of conventional war.” See University of Pennsylvania, Centre for Ethics and the Rule of Law, “Challenging the Grey

- Zone—The Changing Character of Warfare and the Application of International Law,” 3–4 April 2019, <https://www.pennccerl.org/conferences/greyzone/#:~:text=The%20U.S.%20Special%20Operations%20Command,Joseph%20Votel%20et> (accessed 20 January 2022).
- <sup>20</sup> NATO, “NATO 2030.”
- <sup>21</sup> Emily Harding, “The Intelligence Community’s Annual Threat Assessment,” Center for Strategic and International Studies, 19 April 2021, <https://www.csis.org/analysis/intelligence-communitys-annual-threat-assessment> (accessed 21 August 2021).
- <sup>22</sup> Anne-Mari Brady, “China-Solomon Islands Security Treaty—Time for the US to Step Up in Solomon Islands,” *The Diplomat*, 19 April 2022, <https://thediplomat.com/tag/china-solomon-islands-security-treaty/> (accessed 23 April 2022).
- <sup>23</sup> Organization for Economic Cooperation and Development, “The Belt and Road Initiative in the Global Trade, Investment and Finance Landscape,” OECD Business and Finance Outlook 2018 (Paris: OECD Publishing, 2018), [https://doi.org/10.1787/bus\\_fin\\_out-2018-6-en](https://doi.org/10.1787/bus_fin_out-2018-6-en). <https://www.oecd.org/finance/Chinas-Belt-and-Road-Initiative-in-the-global-trade-investment-and-finance-landscape.pdf> (accessed 22 April 2022).
- <sup>24</sup> Magnus Normark, “How States Use Non-State Actors: A Modus Operandi for Covert State Subversion and Malign Networks,” *Strategic Analysis*, Vol. 15 (19 April 2019), p. 2. Also, Paola Tessari and Karolina Muti, “Strategic or Critical Infrastructures, a Way to Interfere in Europe: State of Play and Recommendations.” European Parliament, Directorate-General for External Policies Policy Department, 12 July 2021, p. 23, [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653637/EXPO\\_STU\(2021\)653637\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653637/EXPO_STU(2021)653637_EN.pdf) (assessed 20 January 2022).
- <sup>25</sup> Andrew Radin, Alyssa Demus, and Krystyna Marcinek, “Understanding Russian Subversion—Patterns, Threats, and Responses,” RAND Corporation, February 2020, [https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE331/RAND\\_PE331.pdf](https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE331/RAND_PE331.pdf) (accessed 10 April 2022) and Nick Reynolds and Jack Watling, “Ukraine Through Russia’s Eyes,” *RUSI*, 25 February 2022, <https://rusi.org/explore-our-research/publications/commentary/ukraine-through-russias-eyes> (accessed 10 April 2022).
- <sup>26</sup> Tessari and Muti, “Strategic or Critical Infrastructures, a Way to Interfere in Europe,” p. ix.
- <sup>27</sup> *Ibid.*, p. 23.
- <sup>28</sup> NATO, “Hybrid Definition. NATO Headquarters,” *Lawfas* (2021), [https://lawfas.hq.nato.int/HW/SitePages/Hybrid\\_4.aspx](https://lawfas.hq.nato.int/HW/SitePages/Hybrid_4.aspx) (accessed 28 January 2022; not available to the public). For a historical and developmental overview of hybrid warfare, threats, grey zone, and unrestricted warfare, see Sascha-Dominik Bachmann, Vladimir Oliver, Andrew Dowse, and Hakan Gunneriusson, “Competition Short of War—How Russia’s Hybrid and Grey-Zone Warfare are a Blueprint for China’s Global Power Ambitions,” *Australian Journal of Defence and Strategic Studies*, Vol. 1, No. 1 (2019), pp. 41–56.
- <sup>29</sup> van Cleave, “Counterintelligence and National Security,” p. 4.
- <sup>30</sup> Covert action is described in detail by William J. Daugherty, “The Role of Covert Action,” in *Handbook of Intelligence Studies*, edited by Loch K. Johnson (Oxon: Routledge, 2007), Part 5, pp. 279–288; William J. Daugherty,

- The Role of Covert Action: Executive Secrets—Covert Action and the Presidency* (Lexington: The University Press of Kentucky), pp. 48–57; John Prados, “The Future of Covert Action,” in *Handbook of Intelligence Studies*, edited by Loch K. Johnson (Oxon: Routledge, 2007), Part 5, pp. 289–298 and Mark M. Lowenthal, *Intelligence—From Secrets to Policy* (Thousand Oaks, CA: CQ Press, 2008).
- <sup>31</sup> European Union Agency for Cybersecurity (ENISA), “Threat Landscape Report 2018—15 Top Cyberthreats and Trends,” *European Union Agency for Network and Information Security* (January 2019), p. 126. doi:10.2824/967192 (accessed 1 February 2022).
- <sup>32</sup> *Ibid.*, p. 126.
- <sup>33</sup> Kyle Fendorf and Jessie Miller, “Tracking Cyber Operations and Actors in the Russia-Ukraine War,” *Council on Foreign Relations*, 24 March 2022, <https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war> (accessed 22 April 2022) and Joel Schectman and Christopher Bing, “EXCLUSIVE: Ukraine Calls on Hacker Underground to Defend against Russia,” *Reuters*, 25 February 2022, <https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/> (accessed 22 April 2022).
- <sup>34</sup> See reference 30.
- <sup>35</sup> Tessari and Muti, “Strategic or Critical Infrastructures, a Way to Interfere in Europe,” pp. 23–24.
- <sup>36</sup> NATO, “NATO 2030.”
- <sup>37</sup> *Ibid.*, p. 16.
- <sup>38</sup> *Ibid.*, p. 9.
- <sup>39</sup> NATO, *Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*, 25 August 2010, [https://www.act.nato.int/images/stories/events/2010/20100826\\_bi-sc\\_cht.pdf](https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf) (accessed 12 May 2022).
- <sup>40</sup> NATO, “NATO 2030,” p. 16.
- <sup>41</sup> *Ibid.*, p. 2.
- <sup>42</sup> *Ibid.*
- <sup>43</sup> Hank Prunckun is an authority on counterintelligence. See his contribution to such theory and practice at World Cat Identities, <http://worldcat.org/identities/lccn-n87921195/> (accessed 15 April 2022). A significant publication in this regard is Hank Prunckun, *Counter-Intelligence Theory and Practice*, 2nd ed. (New York: Rowman & Littlefield, 2019).
- <sup>44</sup> “A longer, classified version of the document that describes threats in greater detail is distributed to the congressional intelligence committees, the heads of relevant agencies and officials with appropriate security clearances at the White House, among others.” See Olivia Gazis, “U.S. Counterintelligence Chief Warns of Broadening Spy Threat,” *CBS News*, 10 February 2020, <https://www.cbsnews.com/news/u-s-counterintelligence-chief-warns-of-broadening-spy-threat/> (accessed 10 February 2022).
- <sup>45</sup> United States, “National Counterintelligence Strategy of the United States of America 2020–2022,” p. 2.
- <sup>46</sup> *Ibid.*, p. 2.
- <sup>47</sup> *Ibid.*, pp. 2–3.

- 48 Emily Harding, deputy director and senior fellow with the International Security Program at the Center for Strategic and International Studies (CSIS), in discussion with Karen Greenberg, the author of *Subtle Tools: The Dismantling of American Democracy from the War on Terror to Donald Trump* (Princeton, NJ: Princeton University Press, 2021), and Seth Jones, Harold Brown chair and director of the International Security Program at CSIS. See Emily Harding, “The Deeper Consequences of the War on Terror,” Center for Strategic and International Studies, 19 August 2021, <https://www.csis.org/events/deeper-consequences-war-terror> (accessed 21 August 2021).
- 49 Control Risks, “Cyber Threats in 2020 and beyond Nordic Strategic Outlook,” Control Risks Group Limited, 9 December 2020, <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 9 February 2022).
- 50 Gazis, “U.S. Counterintelligence Chief Warns of Broadening Spy Threat.”
- 51 “The Taiwan Question and Reunification of China,” Taiwan Affairs Office & Information Office of the State Council, the People’s Republic of China, August 1993, Beijing, <http://www.china.org.cn/english/taiwan/7953.htm> (accessed 15 November 2021).
- 52 Harding, “The Deeper Consequences of the War on Terror.”
- 53 *Ibid.*
- 54 *Ibid.*
- 55 C. Textor, “Selected Countries with the Largest Number of Overseas Chinese 2020,” *Statista*, 25 January 2022, <https://www.statista.com/statistics/279530/countries-with-the-largest-number-of-overseas-chinese/> (accessed 15 April 2022).
- 56 Harding, “The Deeper Consequences of the War on Terror.”
- 57 Tessari and Muti, “Strategic or Critical Infrastructures, a Way to Interfere in Europe,” pp. 28–29.
- 58 *Ibid.*, p. 29.
- 59 Barnea, “Counterintelligence,” p. 28.
- 60 Eisenkot and Siboni, “Guidelines for Israel’s National Security Strategy,” p. 21.
- 61 Barnea, “Counterintelligence,” p. 28.
- 62 Eisenkot and Siboni, “Guidelines for Israel’s National Security Strategy,” p. 20.
- 63 Barnea, “Counterintelligence,” p. 28.
- 64 Eisenkot and Siboni, “Guidelines for Israel’s National Security Strategy,” p. 20 and 24.
- 65 “[Cyber] threat agents’ groups: cyber-criminals, insiders, cyber-spies, hacktivists, cyber-offenders, cyber-fighters, cyber-terrorists and script-kiddies.” See ENISA, “Threat Landscape Report 2018—15 Top Cyberthreats and Trends,” p. 119.
- 66 Eisenkot and Siboni, “Guidelines for Israel’s National Security Strategy,” p. 20.
- 67 Tessari and Muti, “Strategic or Critical Infrastructures, a Way to Interfere in Europe,” p. 25.
- 68 Control Risks, “Cyber Threats in 2020 and beyond Nordic Strategic Outlook.”
- 69 SAIIA, “Vaccine Diplomacy and Beyond: New Trends in Chinese Image-Building in Africa,” South African Institute of International Affairs, 22 July 2021, <https://saiia.org.za/research/vaccine-diplomacy-and-beyond-new-trends-in-chinese-image-building-in-africa/> (accessed 15 November 2021).

- <sup>70</sup> Tessari and Muti, pp. 29–30.
- <sup>71</sup> *Ibid.*, p. 29.
- <sup>72</sup> Rebecca Arcesati, “China’s Digital Silk Road and Undersea Cables: Prospects and Threats Posed to the EU,” German Marshal Fund Online Event, 19 March 2021. Retrieved from “China’s Digital Silk Road and Undersea Cables: Prospects and Threats Posed to the EU,” <https://www.youtube.com/watch?v=iPCKZQ8p7uM> (accessed 3 February 2022), in Tessari and Muti, “Strategic or Critical Infrastructures, a Way to Interfere in Europe,” p. 17.
- <sup>73</sup> Rebecca Arcesati’s research focuses on China’s digital and technology policies and how they impact Europe. She covers digital infrastructure and the global expansion of Chinese tech firms, data, and emerging tech governance issues, as well as European Union–China relations in the technology and innovation spaces. Rebecca Arcesati, “Analyst,” *Merics*, <https://merics.org/en/team/rebecca-arcasati> (accessed 16 April 2022).
- <sup>74</sup> Arcesati, “China’s Digital Silk Road and Undersea Cables,” p. 17.
- <sup>75</sup> *Ibid.*, p. 17.
- <sup>76</sup> David B. Larter, “The US Navy Returns to an Increasingly Militarized Arctic,” *defencenews*, 12 May 2020, <https://www.defensenews.com/naval/2020/05/11/the-us-navy-returns-to-an-increasingly-militarized-arctic/> (accessed 15 November 2021).
- <sup>77</sup> Tessari and Muti, “Strategic or Critical Infrastructures, a Way to Interfere in Europe,” p. 25.
- <sup>78</sup> “Nordic countries” refers to Denmark, Finland, Iceland, Norway, and Sweden, which have varying status in NATO and the EU but their own defense cooperation. See Nordic Defence Cooperation, <https://www.nordefco.org/default.aspx> (accessed 10 December 2021).
- <sup>79</sup> Control Risks, “Cyber Threats in 2020 and beyond Nordic Strategic Outlook.”
- <sup>80</sup> *Ibid.*
- <sup>81</sup> Phelan Chatterjee, “Are Sweden and Finland Going from Neutral to NATO?,” *BBC News*, 11 May 2022, <https://www.bbc.com/news/world-europe-61397478> (accessed 12 May 2022).
- <sup>82</sup> Control Risks, “Cyber Threats in 2020 and beyond Nordic Strategic Outlook.”
- <sup>83</sup> *Ibid.*
- <sup>84</sup> *Ibid.*
- <sup>85</sup> South Africa, “South African National Strategic Intelligence Act 39 of 1994,” [https://www.gov.za/sites/default/files/gcis\\_document/201409/act39of1994.pdf](https://www.gov.za/sites/default/files/gcis_document/201409/act39of1994.pdf) (accessed 10 February 2022).
- <sup>86</sup> Jane Duncan, “South Africa’s Tipping Point: How the Intelligence Community Failed the Country,” *Daily Maverick*, 14 July 2021, <https://www.dailymaverick.co.za/article/2021-07-14-south-africas-tipping-point-how-the-intelligence-community-failed-the-country/> (accessed 15 February 2022), as well as Farouk Araj, “Intelligence Failure on Co-Ordinated Insurrection will Cost South Africa Billions,” *Mail and Guardian*, 13 July 2021, <https://mg.co.za/opinion/2021-07-13-intelligence-failure-on-co-ordinated-insurrection-will-cost-south-africa-billions/> (accessed 15 February 2022).
- <sup>87</sup> Tessari and Muti, “Strategic or Critical Infrastructures, a Way to Interfere in Europe,” p. 30.
- <sup>88</sup> *Ibid.*, pp. 30–31.



- <sup>89</sup> “It is a threat posed to [...] national security by someone who misuses or betrays, wittingly or unwittingly, their authorized access to any [government] resource. This threat can include damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.” See United States, “National Insider Threat Task Force Mission Fact Sheet,” Office of the Director of National Intelligence, [https://www.dni.gov/files/NCSC/documents/products/National\\_Insider\\_Threat\\_Task\\_Force\\_Fact\\_Sheet.pdf](https://www.dni.gov/files/NCSC/documents/products/National_Insider_Threat_Task_Force_Fact_Sheet.pdf), accessed 16 February 2022. This is a U.S. government definition, but applicable to any other government or organization.
- <sup>90</sup> United States, “National Counterintelligence Strategy of the United States of America 2020–2022,” p. 3.
- <sup>91</sup> ENISA, “Threat Landscape Report 2018,” p. 120.
- <sup>92</sup> Control Risks, “Cyber Threats in 2020 and beyond Nordic Strategic Outlook.”
- <sup>93</sup> ENISA, “Threat Landscape Report 2018,” p. 124.
- <sup>94</sup> Launched in 2014, One Belt One Road (一帶一路), presented internationally as the Belt and Road Initiative, is China’s signature vision for reshaping its global engagements. See Paul Nantulya, “Implications for Africa from China’s One Belt One Road Strategy,” Africa Centre for Strategic studies, 22 March 2019, <https://africacenter.org/spotlight/implications-for-africa-china-one-belt-one-road-strategy/> (accessed 20 February 2022).
- <sup>95</sup> Nantulya, “Implications for Africa from China’s One Belt One Road Strategy.”
- <sup>96</sup> *Ibid.*
- <sup>97</sup> Josh Fruhlinger, “What is IoT? The Internet of Things Explained,” *Networkworld*, 13 May 2020, <https://www.networkworld.com/article/3207535/what-is-iot-the-internet-of-things-explained.html> (accessed 5 February 2022).
- <sup>98</sup> Oracle, “What is IoT?” (2022), <https://www.oracle.com/za/internet-of-things/what-is-iot/> (accessed 18 February 2022).
- <sup>99</sup> *Ibid.*
- <sup>100</sup> Nisha Talagala, “Don’t Worry about the AI Singularity: The Tipping Point is Already Here,” *Forbes*, 21 June 2021, <https://www.forbes.com/sites/nishatalagala/2021/06/21/dont-worry-about-the-ai-singularity-the-tipping-point-is-already-here/> (accessed 1 February 2022).
- <sup>101</sup> David, C. Martin, *Wilderness of Mirrors* (New York: Harper Collins, 2018).
- <sup>102</sup> Oracle, “What is IoT?”
- <sup>103</sup> Euromoney Learning, “What is Blockchain?” *Euromoney* (2022), <https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain> (accessed 4 February 2022).
- <sup>104</sup> Hank Prunckun, *Counter-Intelligence Theory and Practice*, 2nd ed. (New York: Rowman & Littlefield, 2019).
- <sup>105</sup> United States, “National Counterintelligence Strategy of the United States of America 2020–2022,” p. 8.