Impact of the Russia–Ukraine War on National Cyber Planning: A Survey of Ten Countries

Greg Austin and Natallia Khaniejo

December 2023

IISS
The International Institute
for Strategic Studies

Contents

Executive Summary

Russia's war against Ukraine has involved the most extensive and continuous use of hostile cyber operations by one state against another in history. As the war has unfolded, cyber operations by both sides have become increasingly prominent, with Russia stepping up cyber attacks on the United States and allied countries. These events have motivated other countries to shore up their capabilities to defend against similar cyber operations in the future.

This paper explores how ten countries – Canada, Finland, France, Germany, Japan, the Netherlands, Poland, Sweden, the United Kingdom and the US – have responded to the war in the cyber domain. Based on analysis of government documents and public statements, combined with a workshop held in Berlin in October 2023, the authors have identified five takeaways from the war.

Firstly, there is a recognition that the blurring of boundaries between competition, crisis and war in cyberspace requires a continuity of cyber defence. Secondly, establishing the foundations for national cyber security should be among a state's top priorities, and this requires continuous budget allocations to maintain it. Building on the basics of good cyber security, the third takeaway is the significance of a broader and more proactive cyber defence informed by the principle of defence 'in depth'. The fourth insight is that national cyber defence is more easily achieved through effective partnerships (between governments and the private sector) and through alliances (with like-minded countries). Finally, influence operations are a growing and significant challenge in cyberspace, with most of the states surveyed introducing new measures to enhance societal resilience against such operations.

The result has been a strong upsurge in institutional reform and budget allocations for cyber missions. Even in countries where the trajectory of policy reform and investment was already quite pronounced before 2022 (such as in the US and the UK), important organisational adjustments have been announced, alongside marked increases in budget allocation and modest to large-scale expansion of human resources dedicated to particular cyber missions.

Countries like Japan have realised that a more proactive approach to cyber defence is an inescapable reality, and they are actively seeking ways to incorporate it into their doctrine in a transparent manner. However, in some European countries such as France, Germany and the Netherlands, a more proactive approach to cyber defence is contentious, as it could be perceived as potentially aggressive. Nevertheless, the United States' concept of 'persistent engagement', including 'hunt-forward' operations, has growing appeal. All of the countries reviewed have refined or stepped up the restructuring of their cyber military assets, not only for warfighting but also to ensure that in peacetime the military elements reinforce continuous national cyber defence.

The cyber defence of Ukraine has shown the importance of alliances. Many countries have therefore enhanced their cyber diplomacy by fostering, expanding and deepening partnerships. The American and British view of a more proactive approach to achieving continuity of cyber defence is likely to be progressively adopted by more countries, especially their close allies.

The war has underlined the role of tech companies as geopolitical actors, since they have made decisive interventions in the war. Firstly, the direct provision by these firms of cyber-security services and capabilities has buttressed Ukraine's cyber defence at critical moments. Secondly, tech companies have brought down Russia's economic and reputational standing by curtailing operations in the country following the invasion. However, some countries, especially the US, UK and EU members, have raised a number of political concerns around the quasi-combatant role of these private corporations in relation to the principles of international humanitarian law.

Influence operations have become a much more important focal point of policy as the Russian and

Ukrainian governments (along with their respective state and non-state supporters) have fought to control the narrative surrounding the war and its progress. While information warfare of this kind is not a novel concept or doctrine, cyber capabilities enable it to be executed on a greater scale than what was previously possible. Some countries surveyed, such as Sweden, have invested in new government bodies to lead in this area, while Poland has increased investment in this area of policy. Most of the countries surveyed have adopted whole-of-society approaches to defeating information operations. Techniques include partnering with platforms to introduce greater transparency and accountability mechanisms; educational initiatives to promote digital literacy; increased calls for the attribution of information operations; the use of cyber operations to disrupt information operations; and working through alliances to counter information operations. However, only a few of the countries surveyed are carrying out all of these measures, since most do not attribute information operations.

Overall, most of the countries in this study have made significant adjustments to national-security policies and cyber-policy planning. As a result, the profile of national cyber capabilities is poised to become even more prominent than it is today. China's cyber operations and potential will become an important additional motivation to bolster national cyber defence. The war has in some ways sharpened the will of leading governments to strengthen their commitment to a whole-of-society approach to support national cyber capabilities, defence and resilience. In Finland, this is demonstrated in the government's concept of total national defence.

Further significant adjustments in national cyber policy will continue to be made if Russia continues to expand its cyber and information operations against Ukraine and its allies.

1. Introduction

As Canada's defence minister observed in June 2023, 'Putin's war on Ukraine has reminded all of us that the cyber domain is crucial to our national security'.[1] This paper surveys ten countries to understand how they have understood the impact of the cyber operations in the Russia–Ukraine war. We look at Canada, Finland, France, Germany, Japan, the Netherlands, Poland, Sweden, the United Kingdom and the United States.

This research draws on statements of strategic policy, including announced shifts on doctrine, force structure, workforce development and spending. The analysis is also based on the outcomes of a workshop held in Berlin in October 2023. The authors take a broad view of strategy and operations for the cyber domain, recognising that many of the relevant polices and capabilities are not military-owned and that cyber security in particular requires a whole-of-society approach. The paper does not cover the full gamut of the national-security aspects of cyberspace such as shaping national industry policy.

While a key reference point for this paper is Russia's full-scale invasion of Ukraine on 24 February 2022, the authors also recognise that most of the states covered in this report had already been upgrading their cyber postures in response to increasing cyber threats from Moscow and other actors such as Beijing for over a decade prior. In addition, while some of the announcements for cyber upgrades following the invasion were prepared before the invasion itself, the war has underlined the importance of specific cyber defence and resilience measures for many of the countries, and these are highlighted in this research.

2. Continuity of Cyber Defence

The war has showcased that there is no clear demarcation between peace and war in cyberspace. There is a blurring of the boundaries between competition, crisis and conflict, and countries experience a steady state of at least 'competition' during peacetime. They must therefore plan to build cyber defence and resilience in a manner that accounts for this perpetual state of tension. While many countries surveyed had already recognised prior to February 2022 that increasing cyber security would require further capability investment, the war has added urgency to their efforts. The conflict has also made clear that a purely reactive defensive position in cyberspace does not suffice, and a more forward-leaning approach is required. The blurring of boundaries means that states can benefit by planning (through their strategies and investments) for continuity of cyber defence across the spectrum of conflict.

Some states also have a greater appreciation of the value of adopting a more proactive approach to cyber defence. They base this not only on the strength of Ukrainian cyber defence since February 2022, but also on Kyiv's efforts at bolstering cyber resilience for almost a decade prior to the invasion. For example, Ukraine had already been making significant investments in strengthening its cyber defences since Russia's 2014 annexation of Crimea.[2] Ukraine's experience defending against Russian cyber operations in the past decade has therefore formed a critical component of the country's national cyber resilience.

3. Implementing Basic Cyber Security

A key insight for all ten countries surveyed is the need to improve basic cyber security across the individual and organisational levels, as well as across the public and private sectors. In April 2023, the Five Eyes' national cyber-security organisations jointly published a report on best practices for smart cities identifying risks and providing recommendations.[3] IBM, Microsoft and Nozomi Networks also contributed to this report. The study highlights a changing approach to ensuring cyber hygiene by re-examining and strengthening foundational defences against repeated and targeted cyber attacks during crises. In particular, countries are placing greater emphasis on improving their national cyber resilience, including through the use of regulatory frameworks. Other measures include implementing security by design across all stages of capability development and organisational functions.

Canada has announced plans to boost cyber security. While the country had already identified this area as a significant priority and released its National Cyber Security Strategy in 2018, in its 2022 budget the government earmarked CAD875.2 million for five years starting in the financial year 2022–23.[4] Out of this, CAD252.3m will be invested in making critical government systems more resilient to cyber incidents. The budget also provided for another CAD238.2m (not included in the CAD875.2m mentioned earlier) for additional unspecified measures in response to the evolving threat landscape. Canada announced its intention to establish a cyber-security certification programme to protect its defence supply chain committing CAD25m over three years in an initiative designed with the US Department of Defense.[5]

In its National Strategic Review released in 2022, France laid out cyber resilience as a key strategic priority.[6] In addition, President Emmanuel Macron announced the government's intent to have world-class cyber defence within five years.[7] In November 2023, the government announced a modest commitment of EUR39m for 17 projects intended to bolster cyber resilience. The National Strategic Review noted that despite efforts to boost cyber security, there was still 'significant room for improvement'.[8]

Similarly, while Germany had established a cyber-security centre in 2016, the country recognises that it needs to continue its efforts in this area. In the report titled 'The State of IT Security in Germany 2023', the Federal Office for Information Security (BSI) stated that it needed to 'actively shape cyber security to get "in front of the curve"'.[9] The BSI also noted that since 2020, corporate spending on IT had been increasing steadily, and the figure for this area was EUR7.8 billion in 2022. Despite these investments, German companies suffered a loss of EUR203bn from cyber attacks in 2022, according to the digital association Bitkom. As part of an overarching vision and restructuring of the Federal Ministry of the Interior and Community (BMI), the ministry released in July 2022 the 'Cyber Security Agenda of the Federal Ministry of the Interior and Community'. In that paper, the ministry explicitly stated that the Ukraine war had showed the importance of cyber security for advanced digital economies like Germany that face increased threats through targeted attacks on critical infrastructure and increased cyber-criminal activity.[10]

Japan's 2022 National Security Strategy (NSS) noted the importance of cyber security and resilience, especially in terms of defending critical civilian infrastructure, preventing disinformation and possessing the capabilities to counter information warfare in general.[11] In 2022, Japan also released its updated Cybersecurity Policy for Critical Infrastructure Protection.[12] This document emphasised the need for independent and proactive measures by all stakeholders to make sure they contribute to nurturing a cyber-security-focused culture for the sustainable development of society.[13] While the NSS mentioned Russia's actions as a key trigger for Tokyo's changing security outlook, this shift is motivated more by China.

This is particularly relevant given that Japan's National Center of Incident Readiness and Strategy for

Cybersecurity admitted that it suffered from a security breach which went undetected from October 2022 to June 2023. While the Japanese have not identified China outright as responsible for the October 2022 breach, several sources have made the link, and as a result Japan has committed to boosting its cyber-security budget by a factor of ten over the next five years.[14] This breach came after reports that Japan had 114 ransomware attacks in the first half of 2022, which was an 87% increase over the previous year.[15]

After submitting bids to join NATO, Finland and Sweden revealed their concerns over a rise in cyber attacks and possible Russian retaliation. Finland reported seeing a four-fold spike in ransomware attacks since joining the Alliance.[16] The Nordic countries are also prioritising cyber security as part of improving national cyber defence. Denmark, Finland, Iceland, Norway and Sweden are set to invest a total of USD2bn in upgrading their military and national cyber defences.[17]

In addition, there has been an increase in public–private partnerships, with cyber-security companies forming strategic partnerships with regional armed forces. For example, the Norwegian firm Atea clinched a two-year IT and cyber-security services contract worth USD45m from the Norwegian Defence Research Establishment and the Norwegian National Security Authority.[18] This followed a USD6m contract signed by Finnish software specialist Digia and Danish cyber-security technologies provider Arbit Cyber Defence Systems to build a protected information-exchange gateway for the Finnish Defence Forces. During its half-year EU presidency, Sweden also identified cyber security as a key strategic area.[19]

The UK and the US had considered cyber security a priority before February 2022, so attributing their investments in this area solely to the war would be a misinterpretation. However, the war has definitely bolstered efforts by both countries to adopt a more diversified and holistic approach to the cyber domain.

In its annual cyber-strategy progress report, London announced plans to strengthen its cyber resilience legislation and highlighted how it had supported industry and critical national infrastructure operators facing heightened cyber threats in response to the Russian invasion.[20] It found that 12,000 small businesses had used the National Cyber Security Centre's Cyber Action Plan and over 15,000 had used the 'Check Your Cyber Security' tool. The UK established a National Cyber Advisory Board in 2022, and it also launched in 2023 a Cyber Advisor scheme that aims to provide small and medium enterprises with reliable and cost-effective cyber-security advice and practical support through the application of the technical controls listed in its Cyber Essentials scheme.[21] The National Cyber Strategy 2022 highlighted the UK's commitment to adopting a whole-of-society approach and reinforcing basic cyber hygiene to ensure well-rounded cyber security.[22] While the strategy identified the improvements that had taken place with 77% of businesses responding positively to the government's efforts and identifying cyber security as a key priority, the strategy nevertheless noted that legacy IT systems, supply-chain vulnerabilities and a shortage of cyber-security professionals remained areas of concern.[23]

In the same vein, Washington's National Cybersecurity Strategy 2023 emphasised the need to rebalance cyber-security responsibilities away from vulnerable sections like small businesses and individuals to organisations capable of risk reduction.[24] Prior to the Russia–Ukraine war, the US government had already put out executive orders and memorandums on improving national cyber security, leveraging quantum computing and risk mitigation for vulnerable cryptographic systems, and moving the government towards zero-trust cyber-security principles.[25] The 2023 strategy sought to build on those efforts by securing critical infrastructure through expanding the use of minimum cyber-security requirements in critical sectors, enabling public–private collaboration, as well as defending and modernising federal networks.[26]

4. Cyber Defence in Depth

The US has been a visible proponent of a forward-leaning cyber-defence strategy known as 'persistent engagement' that recognises the need for more than passive cyber defence and sees the value in a greater continuity of cyber defence across the spectrum of conflict. In 2018, the US government formally adopted a policy of 'defending forward' in cyberspace that describes the use of cyber operations to disrupt and degrade adversarial ecosystems.[27] This policy had multiple objectives, including to disrupt or defeat adversary attacks in peacetime without crossing the threshold to armed conflict and, in parallel, to enable US cyber forces to be better prepared to make the transition from peacetime competition to crisis management and beyond to warfighting. The expectation was that this activity would yield valuable new intelligence on adversary systems and technical procedures that the US could exploit more readily than if it had waited for an all-out war to arise.

The US has regarded the outcome of its cyber operations in the war as validation for its strategy of 'persistent engagement' and 'defending forward'.[28] Washington has referenced its collaboration with Ukraine to jointly detect, disable or disrupt a large proportion of Russian cyber operations that had escalated dramatically against Ukrainian military and civil targets in January 2022 as a prelude to the war. While countries recognise that a broader approach to cyber defence that seeks to incorporate whole-of-society security and securitisation against hybrid threats is inescapable, how far the full tenets of US persistence theory and the approach to defend forward is adopted varies between the countries surveyed. The US and its closest allies (such as the UK) are prioritising efforts with a wider range of international partners to add to collective cyber-security capacity, including by taking up a commitment at some level to concepts such as 'defend forward' or 'hunt forward'.

Countries like France and the Netherlands had acknowledged before the war that they possess offensive cyber capabilities and these could help with a 'defend forward' posture. Similarly, Canada has reiterated its intention to continue to develop and scale its offensive cyber capabilities.[29] Prior to the war, Sweden had set up two units to increase robustness for defensive and offensive cyber operations.[30]

Japan has given its introduction of a more proactive approach to cyber defence the label 'active cyber defence' – a term used by many countries but with vastly varying meanings. Japan's 2022 National Security Strategy incorporated this concept with the aim of eliminating 'in advance the possibility of serious cyberattacks that may cause national security concerns' and preventing the 'spread of damage in case of such attacks'.[31] Of special note, the strategy said that this should be used even if the cyber attacks 'do not amount to an armed attack'. The Japanese government also announced it would have to introduce significant legal reforms, including some reinterpretation of a constitutional provision that prohibits government intrusion on the secrecy of private communications.[32]

However, there are concerns regarding this tilt towards more proactive approaches to cyber defence. France, Germany and the Netherlands have publicly stated some concerns about a more forward-leaning defence. In December 2022, the commander of France's Cyber Command expressed reservations about the essentially aggressive character of US hunt-forward operations in spite of their utility.[33] Similarly, the Dutch Defence White Paper 2022 mentioned the role of the Defence Cyber Command in defeating disruptive cyber attacks,[34] but the government policy is limited to allowing such operations in wartime. The 2023 German National Security Strategy carried a similar message: 'We fundamentally reject the idea of using hack-backs as a means of cyber defence.'[35] The Dutch and Germans, however, are likely to keep their options open as both support more proactive approaches to cyber defence, including working with allies. Several European countries are looking for a consensus on the scope of active defence and this will likely be a precondition for establishing new approaches to proactive engagement with hostile cyber campaigns on a continuing basis.[36]

5. Defence Strategy and Plans

Several countries have begun undertaking restructuring efforts aimed at better integrating their cyber abilities with national-security aims and military capabilities. The rationale of this effort is to ensure that the political, military, intelligence and technical aspects of cyber defence are mutually reinforcing.

The US, UK and Japan see such integration as a necessity and an urgent priority. US Deputy Assistant Secretary of Defense for Cyber Policy Mieke Eoyang noted that the Ukraine conflict has most clearly demonstrated the importance of 'integrated cyber capabilities alongside other war fighting capabilities'.[37] Tellingly in September 2023, the US Department of Defense prioritised this integration.[38] In the UK's National Cyber Strategy 2022, London reaffirmed its commitment to developing multidomain operations as laid out in pre-war policy.[39] However, the strategy did not mention Ukraine nor the war specifically. Japan has also given new emphasis to ensuring integrated capabilities in space, cyberspace and electromagnetic domains.[40]

Other countries that have undertaken organisational restructuring include Poland, France and Germany. Poland has been investing in cyberspace defence and cyber security since before the Russian invasion of Ukraine, but the war has made these efforts more urgent and critical. In February 2022, Poland established the Cyberspace Defense Forces modelled on US Cyber Command, and this entity is expected to be operational by 2024.[41] The French Army is setting up a Combat Futures Command to keep pace with the changing nature of warfare and to work towards the integration of the cyber and underwater domains with conventional ones.[42] The Dutch Defence Cyber Command also aims to increase its strike capabilities through deeper integration of its cyber mission teams into multidomain military operations.[43]

Increased defence spending on cyber capabilities, often by large margins, has been a feature of responses to the war. In 2022, Finland along with Austria, France, the Netherlands, Romania and Spain, urged the European Commission to increase cyber-defence spending.[44] These countries called for the EU's Cyber Defence Policy to include not just cyber solidarity in terms of military communication networks, but also a clear blueprint for holistic cyber defence that includes a comprehensive defence technology and industrial base, increased civilian partnership, and voluntary cyber-capacity joint operational development.[45] The countries also called for increased investment in better coordinated cyber defence and a more holistic approach to European cyberspace. The Finnish government has reiterated its goal of accelerating artificial-intelligence security innovation to strengthen national defence. The 2024 national budget aims to increase Finnish cyber defence spending by 30% from its 2023 investment of EUR280m.[46]

The Netherlands' Defence White Paper 2022 foreshadowed an expansion of military cyber personnel from approximately 150 cyber reservists in the Defence Cyber Command by recruiting more than 400 full-time equivalent cyber specialists.[47] In 2023, France announced a 300% increase in funding for military cyber training by 2030.[48] There will also be an increase to 5,000 cyber combatants in the same timeframe.[49]

Sweden's defence budget for 2024 is set to grow by 28% after a substantial increase in 2023 to enable the country to operate effectively with NATO across all domains, including cyber.[50] Under the 2023 budget, the government committed to expanding the capabilities of its Cyber Defence Unit to reinforce its ability to defend against hybrid threats.[51]

As for Japan, its government plans to increase the personnel associated with cyber-related units like the Self-Defense Forces' Cyber Command to 4000 by 2027.[52] By doing so, Tokyo aims to increase the size of the cyber workforce associated with the Ministry of Defense to 20,000.[53] However, while the timing of these measures (announced in December 2022) suggests that these efforts might be related to the war in Ukraine, Japan considers other geopolitical actors such as China to be a greater threat.[54] Beijing, rather than the war, was likely a greater contributing factor to Tokyo's new cyber measures.[55]

6. Alliances and Partnerships

The successful cyber defence of Ukraine during the war has been heavily dependent on cyber-security measures Kyiv took during the preceding decade of cyber competition and conflict with Russia. These included Ukraine bolstering its cyber security through close collaboration with international partners and with the private sector, with a substantial acceleration in such cooperation in the immediate run-up to the Russian invasion and ever since. That acceleration meant many of the most crucial partnerships were often enacted ad hoc and cannot be transferrable elsewhere. A key lesson from the war for other states, therefore, is to build a more structured approach to international partnerships and work with the relevant parts of the private sector during peacetime competition so that they do not have to restructure, reskill and rebuild in the middle of a war.

All the countries reviewed in this report are fully aware of the positive impacts of international collaboration on national cyber defence. These countries also realised the need to implement sustainable and structured collaboration going forward. While there have been numerous admirable examples of allies and technology companies rallying to support Ukraine's cyber defence, other countries cannot rely on this demonstration of sympathy and commitment as a given in the future. A key aspect of this reform, therefore, is anchored around deeper cyber collaboration between countries, particularly for cyber defence and information sharing.

The actions of pro-Russian state and non-state actors have reinforced this need for cyber collaboration. Pro-Kremlin hacktivists have shut down key websites and services in France, Germany and Switzerland.[56] They have also ramped up cyber aggression throughout the course of the war, going after various key entities such as the military, transport services and energy networks.[57] This has reinforced the criticality of cyber defence and, particularly, collaborative defence for European countries and their allies, whose cyber-security architecture has been stress-tested through repetitive and escalatory attacks.

Several countries have found that collaborative cyber defence can be strengthened through cyber exercises which often serve as a trust- and capacity-building measure encouraging deeper international cooperation across a range of activities. Exercises like *Locked Shields* and red teaming, as well as bilateral and trilateral engagements, all serve to foster camaraderie to a certain extent. However, such multifaceted and multinational activities require countries to commit to providing technical experts and participants in a domain which is usually significantly understaffed.

There have been a number of cyber drills held during the course of the Ukraine war that show the collaborative nature of such exercises. For instance, in February 2023, France hosted *ORION* 23, which was the largest military exercise involving French forces in 30 years. It was a multidomain one at that with 14 allied countries participating.[58] Around the same time, the British Army led *Defence Cyber Marvel* 2, the largest military-led cyber exercise in western Europe.[59] The drill was a capstone exercise for a training effort over more than 12 months, and it included more than 750 cyber specialists from various British armed services, government agencies and industry partners. Other countries such as Italy, Japan, Kenya and Oman also took part in *Defence Cyber Marvel* 2. The exercise was more oriented towards individual skills than combined operations by military networks. Japan also believes that collaboration is key to cyber defence, and Tokyo intends to deepen cyber ties with the US in terms of Flexible Deterrent Options, bilateral exercises, joint intelligence, as well as intelligence, surveillance and reconnaissance.[60]

Some of these relationships have extended to joint cyber training, combined planning or coordinated cyber operations. As of mid-2023, the US had conducted more than 50 'hunt-forward' operations on 75 networks partnering with at least 23 countries.[61] In February 2023, Finland, Sweden and the US conducted a trilateral military exercise to bolster cyber defence and ensure cross-domain interoperability.[62] The exercise was aimed at improving information

sharing and best practices regarding the active defence of networks.

The war in Ukraine has demonstrated that alliances and partnerships, particularly for cyber defence, are integral to well-rounded national security and defence. In order to deepen and accelerate partnership channels during crises, it is important for countries to start by ensuring structured collaboration and trust-building during peacetime. While new partnerships between countries could be forged more easily due to the shared sense of vulnerability during wartime, that may not always be the case. Hence, countries would do well to build deeper partnerships with trusted channels of communication in the present to avoid having to resort to reactive ad hoc measures, which would be implemented myopically in the case of a future conflict. The war has demonstrated that it is possible to find novel methods to share critical information and resources without compromising sensitive intelligence methods and sources.

Technology Companies as Critical Partners

While there is an appreciation for the expansion and deepening of alliances between states, the war has also underlined the role of tech companies as geopolitical actors. The private sector has made decisive contributions to the war in two key areas. Firstly, the direct provision of cyber-security capabilities, analytic support, connectivity and data resilience has buttressed Ukraine's position. Secondly, curtailing operations within Russia following the invasion has directly affected Moscow's ICT sector.

In the run-up to Russia's full-scale invasion, Amazon was working with Kyiv to back up government databases to the cloud, and this helped mitigate the damage that would have occurred had the Ukrainian systems been physically destroyed, breached or degraded.[63] Although Amazon, Google, Microsoft and Starlink have provided crucial and timely support to Ukraine during the crisis, their intervention has significantly complicated traditional understandings of what is defined as a combatant under the Law of Armed Conflict (LOAC).

The Ukraine war has also seen a resurgence of hacktivist activity that blurs the line between state-sponsored and voluntary activities. In such circumstances, the application of international law is rendered much more difficult.[64] Lindy Cameron, chief executive of the UK's National Cyber Security Centre, observed that the Russian campaign 'largely failed' because of the application of 'Ukrainian and Western digital expertise within governments and the private sector'.[65] However, countries remain uncertain about these interventions and the knock-on effects they might cause when seen through the framework of the LOAC going forward.

Nonetheless, the review of countries' positions has found that most governments have a new appreciation for the role of technology companies in wartime given the key role the latter have played in cyber defence, resilience and intelligence sharing. The most notable interventions have included participation in cyber operations to defend Ukrainian systems; provision of information and communications technology (ICT) infrastructure like cloud storage or satellites to keep Ukraine connected; and boycotts on the provision of ICT services to Russia. In this conflation of private actor and combatant, however, the safety of industry cannot be guaranteed. In the future, aggressors might look to target companies providing crucial defence support, thereby posing a risk to these firms' employees internationally. This further blurs the already hazy demarcation between peacetime and conflict.

According to one study, as of 10 November 2023, over 1,000 companies had curtailed operations in Russia, and this had contributed to the economic decoupling of Western and other ICT corporations from Russia.[66] In March 2022, Jeremy Fleming, then-director of the UK's Government Communications Headquarters, said: 'We've seen businesses all over the Western world distance themselves from the Russian economy. We've seen technology providers step up to make sure that Ukraine can stay connected, or to address disinformation.' Governments have had to begin 'working with businesses in new and truly collaborative ways'.[67] While many Western technology companies have rallied around Ukraine in an admirable manner, they might be less inclined to do so in the future if there is a greater clash of material interests or the boundary between aggressor and victim is not as clearly defined. A number of governments and many of these technology companies have lauded the benefits of these contributions, but are also wary of the political, financial, legal and operational challenges to sustainability in the long run and to replicability in the future.[68]

7. Information Operations

Competition in the information space has involved attempts by the Russian and Ukrainian governments and their non-state supporters to control the narrative surrounding the war and its progress.[69] This includes the spread of disinformation, misinformation, rumours and propaganda. While information warfare is not novel, cyber capabilities enable it to be carried out on a greater scale and scope than what was previously possible.[70] States' use of artificial intelligence, bots and social media to control the narrative has made the proliferation of misinformation, propaganda, rumours and disinformation rampant. The information space has emerged as a key area for competition as well as a significant vulnerability for many of the countries surveyed. This section will examine how countries have introduced various measures to build societal resilience against cyber-enabled information operations.

Many of the countries included in this study had identified the psychological- or political-warfare dimension of disinformation and information operations by Russia before the invasion. Finland, Poland and Sweden had spoken about the increase of Russian information operations and the threat these actions pose to their national security and regional stability.[71] These countries had characterised information operations as sufficiently important in their own right to warrant significant new expenditure and institutional attention. What follows are some examples of national efforts to enhance societal cognitive resilience, which include having dedicated government resources; increasing digital literacy; fact-checking; myth-debunking initiatives; and cyber operations to disrupt adversary's information operations.

In January 2022, Sweden established under its defence ministry the Psychological Defence Agency, which emphasises military defence and civilian resilience.[72] The agency is funded at SEK8m per year from 2024 to 2026, and will have 45 personnel.[73] Similarly, noting the 'prominence of the information front', the UK set up the Government Information Cell in early January 2022 to counter Russian propaganda and disinformation.[74] The British government also released a countering disinformation toolkit called RESIST, which stands for Recognise mis- and disinformation, Early warning, Situational insight, Impact analysis, Strategic communication and Tracking effectiveness to enable governments to more easily communicate threats to their audiences through outcomes and case studies.[75]

Finland has committed to bolstering its communication networks to ensure its citizens have access to necessary authoritative information in the event of serious incidents and emergency conditions.[76] In addition, the Finnish government has a clear communications strategy through which authorities pledge to provide information with objectives and impacts clearly described. Finland ranked first out of 41 European countries in a 2022 survey measuring resilience against misinformation, and this accolade was partially attributed to the national education system teaching Finnish students to identify fake news at a young age.[77]

Since the 2016 US presidential elections, Washington has been aware of the potential for Russian interference in its information environment and democratic processes. While at home the US has relied on tech companies to de-platform Russian propaganda, its approach to countering disinformation has been to increase global information sharing with various US government agencies playing a key role in the process.[78] For example, the US Department of State released in November 2023 a media note regarding Russia's disinformation campaign in Latin America that relied on media contacts to garner support and foster anti-US and anti-NATO sentiments.[79] Similarly, the Department of State's Global Engagement Center has also issued a press release on disarming disinformation.[80] In the same vein, the US Cyber Command and the Cybersecurity and Infrastructure Security Agency have released guides on how to identify adversarial propaganda.[81] The Cyber Command has also led cyber operations to identify Russian troll farms and block them as part of

election defence, an activity underway since at least the 2018 mid-term elections. In 2022, following the invasion of Ukraine, Cyber Command chief General Paul Nakasone confirmed that the US had undertaken cyber operations to dismantle Russian disinformation infrastructure, including in Ukraine.[82]

The value of alliances in defending against information operations prompted the establishment of the NATO Strategic Communications Centre of Excellence (StratCom COE) in 2014 with seven member states: Estonia, Germany, Italy, Latvia, Lithuania, Poland and the UK.[83] Even non-NATO member Australia joined the COE in 2022.[84] The G7 also set up a Rapid Response Mechanism for information sharing and best practices to counter influence operations.[85] In December 2022, the European External Action Service (EEAS) launched a new platform called the Information Sharing and Analysis Centre as part of its efforts to counter disinformation campaigns by Russia and China.[86] Two months later, the service released the first EEAS Report on Foreign Information Manipulation and Interference Threats.[87]

The EU and Canada have attributed and imposed sanctions on the individuals and entities behind Russian information operations. In 2023, the European Council called out Moscow for its information manipulation, and listed seven individuals and five entities responsible for conducting digital information manipulation campaigns under the alias of Recent Reliable News.[88] Canada has been very proactive in its diplomacy against disinformation, imposing sanctions on people seen as complicit in spreading Russian disinformation.[89] Like the attribution for cyber operations, attribution when it comes to information operations while imperfect does at least set a threshold for what qualifies as responsible versus irresponsible behaviour in cyberspace.

Information operations by Russia and other actors are a clear threat to the countries surveyed in this research. To be sure, many efforts to counter these operations preceded Russia's invasion or are related to the prospect of electoral interference in 2024.[90] However, the war in Ukraine has definitely served as an inflection point underlining the criticality of countering disinformation for most countries. To build societal cognitive resilience, governments are not only creating new internal units to lead on this work, but also adopting a whole-of-society approach through partnering with platforms to introduce greater transparency and accountability mechanisms to information systems. Authorities are also driving educational initiatives to promote digital literacy, as well as attributing information operations and working through alliances to counter information operations.

8. Implications

The US and its key allies, including Japan, are mobilising robustly for new capabilities in cyberspace. Some of the targets for growth are ambitious and may well prove to be unreachable for individual countries. Budgets and the availability of skilled workers will likely not match the new goals in most countries. It is highly likely therefore that countries in the US-led alliances and other groupings, such as the EU, will seek to strengthen alliance structures for even more collaborative cyber defence to compensate for their own shortcomings.

The profile of national cyber security will continue to become even more prominent in national-security policy than it is today. It is likely that in the countries most affected by Russia's cyber operations, there will be even greater interest in the ways in which the armed forces can be organised to support national cyber defence.

As long as Russia continues its illegal war or its illegal occupation of Ukraine, the prospects for escalation of cyber operations, including for influence-seeking or psychological effects, will remain. Even if Russia ended the war and was forced to withdraw from Ukraine, the high-intensity cyber and information war between Russia and the West would likely continue.

Apart from Ukraine and Russia which are at war, the protagonists will try to keep the level of cyber activities below the threshold of armed conflict. There may be incentives for Russia to test the limits of that cyber threshold for the US or its allies as a preferred substitute for more serious escalation in diplomatic or military actions. As long as Russia continues to suffer major setbacks in the war, the cyber confrontation will remain unstable and have the potential to become more dangerous. If that happens, we can expect to see an additional round of responses in national cyber policy by the states surveyed in this report.

Notes

1 Government of Canada, 'Remarks From Minister Anand at CANSEC 2023', 5 June 2023, https://www.canada.ca/en/department-national-defence/news/2023/06/remarks-from-minister-anand-at-cansec-2023.html. Similar announcements underlining the importance of cyber security in the face of contemporary threats were announced by other countries. For the US, see US Department of Defense, '2023 Cyber Strategy', 2023, https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF. For the Netherlands, see Netherlands Government, 'Security Strategy for the Kingdom of the Netherlands', 2023, https://www.government.nl/binaries/government/documenten/publications/2023/04/03/security-strategy-for-the-kingdom-of-the-netherlands/Security+Strategy+for+the+Kingdom+of+the+Netherlands.pdf.

2 Isabel Schmidt, Avery Parsons Grayson and Mayesha Alam, 'Cross-Cutting Responses to Strengthen Ukraine's Digital Resilience', Digital Frontlines, 28 June 2023, https://digitalfrontlines.io/2023/06/28/cross-cutting-responses-to-strengthen-ukraines-digital-resilience/.

3 United States Cybersecurity and Infrastructure Security Agency, United States National Security Agency, United States Federal Bureau of Investigation, United Kingdom National Cyber Security Centre, Australian Cyber Security Centre, Canadian Centre for Cyber Security and New Zealand National Cyber Security Centre, 'Cybersecurity Best Practices for Smart Cities', 19 April 2023, https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf.

4 Department of Finance Canada, '2022 Budget', 2022, p. 136, https://nationalpost.com/news/politics/canada-federal-budget-2022-full-text.

5 Government of Canada, 'Government of Canada Helping Defence Industry Protect Itself From Cyber Security Threats', 31 May 2023, https://www.canada.ca/en/public-services-procurement/news/2023/05/government-of-canada-helping-defence-industry-protect-itself-from-cyber-security-threats.html.

6 Republic of France, 'National Strategic Review 2022', 2022, pp. 39–40, https://www.sgdsn.gouv.fr/files/files/rns-uk-20221202.pdf.

7 Elise Vincent, 'Macron Wants "World-class Cyber Defense" for France Within Five Years', *Le Monde*, 11 November 2022, https://www.lemonde.fr/en/international/article/2022/11/11/emmanuel-macron-wants-world-class-cyber-defense-for-france-within-five-years_6003801_4.html.

8 Republic of France, 'National Strategic Review 2022', p. 39.

9 Federal Office for Information Security, 'The State of IT Security in Germany 2023', November 2023, p. 5, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2023.pdf?__blob=publicationFile&v=7.

10 *Ibid*., p. 5.

11 Ministry of Defense, 'National Security Strategy', December 2022, pp. 18, 23, https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf.

12 Government of Japan, 'The Cybersecurity Policy for Critical Infrastructure Protection', June 2022, https://www.nisc.go.jp/eng/pdf/cip_policy_2022_eng.pdf.

13 *Ibid*., p. 2.

14 Graham Cluley, 'Japan's Cybersecurity Agency Admits It Was Hacked for Months', Bitdefender, 30 August 2023, https://www.bitdefender.com/blog/hotforsecurity/japans-cybersecurity-agency-admits-it-was-hacked-for-months/.

15 *Japan Times*, 'Japan Saw 87% Increase in Ransomware Attacks in First Half of 2022', 15 September 2022, https://www.japantimes.co.jp/news/2022/09/15/national/crime-legal/ransomeware-attacks-rise/.

16 Alexander Martin, 'Finland Sees Fourfold Spike in Ransomware Attacks Since Joining NATO, Senior Cyber Official Says', The Record, 3 August 2023, https://therecord.media/finland-sees-fourfold-spike-in-rasomware-attacks-nato.

17 Gerard O'Dwyer, 'Nordic Firms Ride Wave of Cyber M&A Activity', Defense News, 4 July 2023, https://www.defensenews.com/industry/2023/07/04/nordic-firms-ride-wave-of-cyber-ma-activity/.

18 *Ibid*.

19 Gerard O'Dwyer, 'Sweden Vows to Push Defense Collaboration, Cyber Defense at EU Helm', Defense News, 6 January 2023, https://www.defensenews.com/global/europe/2023/01/06/sweden-vows-to-push-defense-collaboration-cyber-defense-at-eu-helm/.

20 Cabinet Office, 'National Cyber Strategy 2022 Annual Progress Report 2022-2023', 14 August 2023,

https://www.gov.uk/government/publications/national-cyber-strategy-2022-annual-progress-report-2022-2023/national-cyber-strategy-2022-annual-progress-report-2022-2023-html.

21 National Cyber Security Centre, 'Cyber Advisor', https://www.ncsc.gov.uk/schemes/cyber-advisor; and National Cyber Security Centre, 'About Cyber Essentials', https://www.ncsc.gov.uk/cyberessentials/overview.

22 Her Majesty's Government, 'National Cyber Strategy 2022: Pioneering a Cyber Future With the Whole of the UK', 2022, pp. 14, 35, 67, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf.

23 *Ibid*., p. 23.

24 The White House, 'National Cybersecurity Strategy', March 2023, p. 4, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

25 The White House, 'Executive Order on Improving the Nation's Cybersecurity', 12 May 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; and Executive Office of the President, 'Memorandum for the Heads of Executive Departments and Agencies', 26 January 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

26 The White House, 'National Cybersecurity Strategy', pp. 6, 7, 9, 10, 15.

27 US Cyber Command, '2023 Posture Statement of Paul M. Nakasone', 7 March 2023, https://www.cybercom.mil/Media/News/Article/3320195/2023-posture-statement-of-general-paul-m-nakasone/.

28 US Department of Defense, 'Cyber Strategy', pp. 2, 9.

29 Government of Canada, 'Standing Senate Committee on National Security, Defence and Veterans Affairs (SECD) - Arctic Security', 24 April 2023, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/proactive-disclosure/secd-april-24-2023/cybercapabilities.html.

30 Swedish Armed Forces, '*Nytt it-försvarsförband stärker Sveriges cyberförsvarsförmåga*' [New IT Defence Unit Strengthens Sweden's Cyber-defence Capabilities], 12 January 2022, https://www.forsvarsmakten.se/sv/aktuellt/2022/01/nytt-it-forsvarsforband-starker-sveriges-cyberforsvarsformaga/.

31 Ministry of Defense, 'National Security Strategy', p. 23.

32 *Yomiuri Shimbun*, 'Active Cyber Defence Framework Could One Day Protect Japan', 14 September 2022, https://asianews.network/active-cyber-defence-framework-could-one-day-protect-japan/.

33 National Assembly, '*Compte rendu Commission de la défense nationale et des forces armées*' [Transcript of the Committee on National Defence and the Armed Forces], 7 December 2022, p. 8, https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/cion_def/l16cion_def2223027_compte-rendu.pdf.

34 Ministry of Defence, 'A Stronger Netherlands, a Safer Europe Investing in a Robust NATO and EU 2022 Defence White Paper', 2022, p. 52, https://english.defensie.nl/binaries/defence/documenten/publications/2022/07/19/defence-white-paper-2022/Defence+White+Paper+2022.pdf.

35 Federal Government, 'Robust. Resilient. Sustainable. Integrated Security for Germany. National Security Strategy, 2023', p. 62, https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf.

36 See Annegret Bendiek and Jakob Bund, 'Shifting Paradigms in Europe's Approach to Cyber Defence', 25 September 2023, p. 3, https://www.swp-berlin.org/publications/products/comments/2023C48_Europe_CyberDefence.pdf.

37 Jeff Seldin, 'Offense is the New Defense in Pentagon's Revamped Cyber Strategy', Voice of America, 12 September 2023, https://www.voanews.com/a/offense-is-the-new-defense-in-pentagon-s-revamped-cyber-strategy/7266028.html.

38 US Department of Defense, '2023 Cyber Strategy', p. 3.

39 Ministry of Defence, 'Integrated Operating Concept 2025', 2020, p. 10, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/10014659/Integrated_Operating_Concept_2025.pdf. Integrated Operating Concept 2025 set out the need for a 'transformation of the military instrument, including the need to structure forces to operate that can be adapted at graduated readiness to warfight'. The changes were premised on the need for multidomain operations with emphasis on the 'importance of integration with allies, of the levers of statecraft, and across the five operational domains'.

40 Ministry of Defense, 'National Security Strategy', pp. 18, 27.

41 Wiktor Sędkowski, 'US Cyber Forces as a Model for the Polish Ones', Warsaw Institute, 28 March 2022, https://warsawinstitute.org/us-cyber-forces-model-polish-ones/.

42 Bertrand Toujouse, 'French Land Forces Chief: How France's Army is Transforming for the Modern Era', 25 May 2023, Breaking Defense, https://breakingdefense.com/2023/05/french-army-chief-how-frances-army-is-transforming-for-the-modern-era/. Toujouse was France's army chief when this article was published.

43 Ministry of Defence, '2022 Defence White Paper', July 2022, p. 52, https://english.defensie.nl/binaries/defence/documenten/publications/2022/07/19/defence-white-paper-2022/Defence+White+Paper+2022.pdf.

44 Luca Bertuzzi, 'Six EU Countries Call for Ambitious Cyber Defence Policy, Document', Euractiv, 30 September 2022, https://www.euractiv.com/section/cybersecurity/news/six-eu-countries-call-for-ambitious-cyber-defence-policy-document/.

45 *Ibid*.

46 Gerard O'Dwyer, 'Finnish Government to Bolster Spending on Cyber-AI Defences', Computer Weekly, 7 September 2023, https://www.computerweekly.com/news/366551252/Finish-government-to-bolster-spending-on-cyber-AI-defences.

47 Ministry of Defence, 'A Stronger Netherlands, a Safer Europe Investing in a Robust NATO and EU 2022 Defence White Paper', p. 52.

48 Jean-Marc Manach, '*Les priorités du Comcyber : chiffre, lutte informatique d'influence (L2I) et partage de données*' [ComCyber Priorities: Cryptology, the Struggle for Cyber Influence and Information Sharing], Next Impact, 4 May 2023, https://www.nextinpact.com/article/71604/les-priorites-comcyber-chiffre-lutte-informatique-dinfluence-l2i-et-partage-donnees.

49 *Ibid.*

50 Lee Ferran, 'Sweden Aims to Boost Military Spending by Nearly 30%, Hitting NATO Spending Target', Breaking Defense, 12 September 2023, https://breakingdefense.com/2023/09/sweden-aims-to-boost-military-spending-by-nearly-30-hitting-nato-spending-target/.

51 Gerard O'Dwyer, 'Sweden Boosts Cyber, Defense Spending with NATO in Mind', C4ISRNet, 23 November 2022, https://www.c4isrnet.com/cyber/2022/11/22/sweden-boosts-cyber-defense-spending-with-nato-in-mind/.

52 Ministry of Defense, 'Defense Buildup Program', pp. 11–12, December 2022, https://www.mod.go.jp/j/approach/agenda/guideline/plan/pdf/program_en.pdf.

53 *Ibid*.

54 Japan's 2022 National Security Strategy identified China, North Korea and Russia as primary threats to its security interests. See Ministry of Defense, 'National Security Strategy', pp. 8–10.

55 In 2023, Japan announced USD75bn being set aside to strengthen cyber capabilities in the Indo-Pacific. Digwatch, 'Japan to Build Cyber Defense Grid for the Indo-Pacific', 31 August 2023, https://dig.watch/updates/japan-to-build-cyberdefense-grid-for-the-indo-pacific.

56 Reuters, 'Russian "Hacktivists" Briefly Knock German Websites Offline', 26 January 2023, https://www.reuters.com/world/europe/russian-hacktivists-briefly-knock-german-websites-offline-2023-01-25/; and AFP, 'Pro-Russian Hackers Claim Downing of French Senate Website', 5 May 2023, https://www.securityweek.com/pro-russian-hackers-claim-downing-of-french-senate-website/.

57 Sean Lyngaas, 'Russian Hackers Targeted European Military and Transport Organizations in Newly Discovered Spying Campaign', CNN, 15 March 2023, https://edition.cnn.com/2023/03/15/politics/russian-hackers-europe-military-organizations-microsoft/index.html.

58 See France in the United Kingdom, 'Orion Exercise Enters Its Last Phase', 19 April 2023, https://uk.ambafrance.org/Orion-2023-military-exercise-enters-its-final-phase. The French defence ministry stated that the exercise's cyber component sought to 'test the effectiveness and coherence' of the Ministry of Armed Forces' chains of command in terms of 'defensive cyber warfare', adding that 'ORION integrates the information environment in order to involve actors of the information warfare and test the coordination of our effects'. See Ministry of the Armed Forces, 'Orion 23 Press Kit', February 2023, p. 11, https://www.defense.gouv.fr/sites/default/files/operations/20230228_Press_Kit_Orion.pdf.

59 British Army, 'Army Leads Western Europe's Largest Cyber Warfare Exercise', 22 February 2023, https://www.army.mod.uk/news-and-events/news/2023/02/defence-cyber-marvel-warfare-exercise/.

60 Ministry of Defense, 'National Security Strategy', p. 22. In 2013, Japan adopted the term 'Flexible Deterrent Options' from standing US policy that sought to strengthen deterrence by swift redeployment of military assets or by other forms of military signalling to convince an adversary of your own side's determination to react with force if necessary.

61 US Cyber Command, '"Building Resilience": U.S. Returns from Second Defensive Hunt Operation in Lithuania', 12 September 2023, https://www.cybercom.mil/Media/News/Article/3522801/building-resilience-us-returns-from-second-defensive-hunt-operation-in-lithuania/.

62 US European Command Public Affairs, 'US, Swedish, Finnish Militaries Join Forces to Defend Cyber Domain', 16 February 2023, https://www.eucom.mil/article/42276/us-swedish-finnish-militaries-join-forces-to-defend-cyber-domain.

63 Amazon, 'Safeguarding Ukraine's Data to Preserve Its Present and Build Its Future', 9 June 2022, https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future.

64 Matt Burgess, 'Hacktivism Is Back and Messier Than Ever', 27 December 2022, Wired, https://www.wired.co.uk/article/hacktivism-russia-ukraine-ddos.

65 National Cyber Security Centre, 'Lindy Cameron at Chatham House Security and Defence Conference 2022', 28 September 2022, https://www.ncsc.gov.uk/speech/lindy-cameron-chatham-house-security-and-defence-conference-2022.

66 Yale School of Management, 'Over 1,000 Companies Have Curtailed Operations in Russia – but Some Remain', 10 November 2023, https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain.

67 National Security College, 'An Address From GCHQ Director Sir Jeremy Fleming', 31 March 2022, https://nsc.crawford.anu.edu.au/department-news/20103/address-gchq-director-sir-jeremy-fleming.

68 See International Committee of the Red Cross, 'Protecting Civilians Against Digital Threats During Armed Conflict. Recommendations to States, Belligerents, Tech Companies, and Humanitarian Organizations', 2023, https://shop.icrc.org/download/ebook?sku=4735/002-ebook.

69 Christian Perez and Anjana Nair, 'Information Warfare in Russia's War in Ukraine', *Foreign Policy*, 22 August 2022, https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/.

70 Brian Babcock-Lumish et al., 'Managing the New Era of Deterrence and Warfare: Visualizing the Information Domain', IBM Center for the Business of Government, Institute for the Study of War, May 2023, p. 6, https://www.businessofgovernment.org/sites/default/files/Managing%20the%20New%20Era%20of%20Deterrence%20and%20Warfare.pdf; and David Calvo et al., 'Countering Disinformation: Improving the Alliance's Digital Resilience', NATO Review, 12 August 2021, https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html.

71 Mariusz Antoni Kamiński and Zdzisław Śliwa, 'Poland's Threat Assessment: Deepened, Not Changed', March 2023, National Defense University Press, 10 March 2023, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3323942/polands-threat-assessment-deepened-not-changed/; Finnish Government, 'Government Report on Finnish Foreign and Security Policy', October 2020, p. 21, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162515/VN_2020_32.pdf?sequence=1&isAllowed=y; and Digwatch, 'Sweden Faces Ongoing Misinformation Campaigns From Russia and Iran, Warns Minister', 29 August 2023, https://dig.watch/updates/sweden-faces-ongoing-misinformation-campaigns-from-russia-and-iran-warns-minister.

72 Steven Lee Myers, 'Sweden Is Not Staying Neutral in Russia's Information War', *New York Times*, 10 August 2023, https://www.nytimes.com/2023/08/10/technology/sweden-combat-disinformation.html.

73 Gerard O'Dwyer, 'NATO Membership to Drive Nordic Cyber Security Sector Growth', Computer Weekly, 18 July 2023, https://www.computerweekly.com/news/366544800/NATO-membership-to-drive-Nordic-cyber-security-sector-growth; and Emma Woolacott, 'Sweden Launches Psychological Defense Agency to Counter Disinformation', Forbes, 5 January 2022, https://www.forbes.com/sites/emmawoollacott/2022/01/05/sweden-launches-psychological-defense-agency-to-counter-disinformation/?sh=566506914874.

74 Government Communication Service, 'Responding to Russia's Invasion', 24 March 2022, https://gcs.civilservice.gov.uk/news/responding-to-russias-invasion/.

75 Government Communication Service, 'RESIST 2 Counter Disinformation Toolkit', 2022, https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/.

76 Publications of the Finnish Government, 'Government Report on Changes in the Security Environment', April 2022, p. 32, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164002/VN_2022_20.pdf?sequence=4&isAllowed=y.

77 Jenny Gross, 'How Finland Is Teaching a Generation to Spot Misinformation', *New York Times*, January 2023, https://www.nytimes.com/2023/01/10/world/europe/finland-misinformation-classes.html.

78 Steven Lee Myers, 'US Tries New Tack on Russian Disinformation: Pre-empting It', *New York Times*, 26 October 2023, https://www.nytimes.com/2023/10/26/technology/russian-disinformation-us-state-department-campaign.html.

79 US Department of State, 'The Kremlin's Efforts to Covertly Spread Disinformation in Latin America', 7 November 2023, https://www.state.gov/the-kremlins-efforts-to-covertly-spread-disinformation-in-latin-america/.

80 US Department of State, 'Disarming Disinformation: Our Shared Responsibility', 20 October 2023, https://www.state.gov/disarming-disinformation/.

81 Dorothy Sherwood, 'Don't Be a Target: How to Identify Adversarial Propaganda', US Cyber Command, 5 October 2023, https://www.cybercom.mil/Media/News/Article/3551070/dont-be-a-target-how-to-identify-adversarial-propaganda/; and Cyber Security and Infrastructure Agency, 'Foreign Information Operations and Disinformation', https://www.cisa.gov/topics/election-security/foreign-influence-operations-and-disinformation.

82 Ines Kagubare, 'Cyber Command Chief Confirms US Took Part in Offensive Cyber Operations', The Hill, 1 June 2022, https://thehill.com/policy/cybersecurity/3508639-cyber-command-chief-confirms-us-took-part-in-offensive-cyber-operations/.

83 NATO Strategic Communications Centre of Excellence, 'About NATO StratCom COE', https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5.

84 Minister for Foreign Affairs, 'Cooperation with NATO's Strategic Communications Centre of Excellence', 7 April 2022, https://www.foreignminister.gov.au/minister/marise-payne/media-release/cooperation-natos-strategic-communications-centre-excellence.

85 Prime Minister of Canada, 'Prime Minister Announces Additional Support for Ukraine', 23 August 2022, https://www.pm.gc.ca/en/news/news-releases/2022/08/23/prime-minister-announces-additional-support-ukraine.

86 Clothilde Goujard, 'EU to Launch Platform to Fight Russian, Chinese Disinformation', Politico, 7 February 2023, https://www.politico.eu/article/eu-to-launch-platform-to-fight-russian-chinese-disinformation/.

87 EEAS, '1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a Framework for Networked Defence', February 2023, https://euvsdisinfo.eu/uploads/2023/02/EEAS-ThreatReport-February2023-02.pdf.

88 European Council, 'Information Manipulation in Russia's War of Aggression Against Ukraine', 28 July 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/07/28/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-seven-individuals-and-five-entities/.

89 Government of Canada, 'Canada's Efforts to Counter Disinformation – Russian Invasion of Ukraine', 22 December 2022, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=eng.

90 See European Parliament, 'Special Committee on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation and the Strengthening of Integrity, Transparency and Accountability in the European Parliament', 23 October 2023, https://www.europarl.europa.eu/committees/en/ing2/home/highlights.

Acknowledgements

IISS–Europe acknowledges the financial support of the German Federal Foreign Office in producing this research paper, including for a workshop that helped inform the paper's contents.

The International Institute for Strategic Studies – UK
Arundel House | 6 Temple Place | London | WC2R 2PG | UK
t. +44 (0) 20 7379 7676 **e.** iiss@iiss.org www.iiss.org

The International Institute for Strategic Studies – Americas
2121 K Street, NW | Suite 600 | Washington DC 20037 | USA
t. +1 202 659 1490 **e.** iiss-americas@iiss.org

The International Institute for Strategic Studies – Asia
9 Raffles Place | #49-01 Republic Plaza | Singapore 048619
t. +65 6499 0055 **e.** iiss-asia@iiss.org

The International Institute for Strategic Studies – Europe
Pariser Platz 6A | 10117 Berlin | Germany
t. +49 30 311 99 300 **e.** iiss-europe@iiss.org

The International Institute for Strategic Studies – Middle East
14th floor, GFH Tower | Bahrain Financial Harbour | Manama | Kingdom of Bahrain
t. +973 1718 1155 **e.** iiss-middleeast@iiss.org