Policy Brief

July 2022

NATO and Societal Resilience: All Hands on Deck in an Age of War

Edward Hunter Christie and Kristine Berzina

Prior to 2022, NATO and the European Union were already moving toward more comprehensive approaches to resilience. Russia's war of aggression against Ukraine heightens the need for such work, with a sharper focus on scenarios of armed attack.

In view of decisions taken at NATO's recent Madrid summit and the evolution of EU legislation, all alliance members will benefit from close liaison work and reciprocal briefings between relevant NATO and European Commission officials as well as through the NATO Resilience Committee and the European Critical Entities Resilience Group.

Three new functions should be added to the NATO baseline requirements: payment systems, psychological defense, and continuity of data and infrastructure software.

The forthcoming membership of Finland and Sweden will provide NATO with particularly valuable national best practices, notably in terms of coherence, robustness, quality of cooperation across government and society, and engagement with the population.

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Washington, DC Ankara Belgrade Berlin Brussels Bucharest Paris Warsaw

Introduction

The ability of societies to withstand and adapt in crises and emergencies is an essential element of national security and defense. As illustrated most sharply by Ukraine's reaction to Russia's invasion, the preparedness of a society, its readiness to sustain sacrifices and hardship, and its will to fight are of paramount importance for national survival and liberty.

NATO's ability to defend itself against an armed attack will likewise depend not only on its military capabilities but also on the preparedness and resilience of its societies. President Vladimir Putin has stated his desire to retake Russia's former imperial territories,[1] and European states face a full spectrum of threats, including economic and natural-resource blackmail, hybrid and terrorist tactics, military intimidation, and wars of aggression and conquest.

Civil preparedness is a long-established area of work for NATO governments.

Civil preparedness is a long-established area of work for NATO governments. Since 2014, the alliance has operationalized its work on resilience through civil preparedness, particularly through its seven baseline requirements that reflect national functions vital to national and collective defense. In this context, the concept of societal resilience has attracted considerable attention in recent years. This brief first discusses key concepts related to preparedness and resilience from a NATO perspective and proposes a definition of societal resilience. It then provides an overview of the European Union's proposed Critical Entities Resilience Directive. The brief then sets out key considerations regarding NATO's baseline requirements for national resilience and their possible evolution, taking into consideration potential complementarities with the EU's approach, as well as early lessons from the war in Ukraine. In light of the Madrid summit decision[2] of June 2022 to invite Finland and Sweden to become members of NATO, we also consider what best practices the alliance could learn from them.

Societal Resilience and National Security

The term resilience is typically defined as the ability of a system to continue to function in times of difficulty and to recover from shocks or crises with minimal disruption. Definitions often posit three phases: preparation, response, and recovery. This implies that resilience is not the result of a single effort or initiative, but rather of a long-term, ongoing effort and investment that changes over time.[3]

From a defense perspective, resilience has been traditionally understood in the context of facing an armed attack. It encompasses not only the ability of armed forces to continue to fulfill their tasks but also the ability of society to resist and recover from attacks so that harm to civilians is mitigated and society can continue to support the needs of armed forces (enablement) and also that military resources are not unduly diverted toward civilian emergencies. Within NATO, this is referred to as civil preparedness, while resilience refers to the combined effect of civil preparedness and military capacity.[4] The pursuit of resilience in the NATO context derives from Article 3 of the Washington Treaty, which states the allies are committed "separately *and jointly* [to] maintain and develop their individual *and collective* capacity to resist armed attack" [emphases added][5]. This implies giving due consideration to the collective level of resilience that is achieved and to avoiding that any ally could become a major point of failure that harms the security of the others.

1 Andrew Roth, "Putin compares himself to Peter the Great in quest to take back Russian lands," The Guardian, June 10, 2022.

2 NATO, Madrid Summit Declaration Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022, June 29, 2022.

3 Ben Caves et al. Enhancing Defense's Contribution to Societal Resilience in the UK: Lessons from International Approaches. RAND Corporation, 2021, p. 7.

4 NATO, Resilience and civil preparedness – Article 3, June 17, 2022.

5 Ibid.

In recent years, a growing realization of the more interconnected and less centralized nature of Western societies has led to increased discussions on the concept of societal resilience. This refers to the ability of communities or society to, at a minimum, "respond to shocks, absorb them without suffering from severe fractures, and then recover."[6] The aim in terms of recovery, which is not always clearly expressed, is not just to recover toward the initial state but also to learn from the shocks and build back better so as to experience less harm should these shocks reoccur.

In practice, the enablement part of resilience remains largely in the hands of civilian public bodies and major corporations that can feasibly be subject to civilian or military authorities, as appropriate.

Societal resilience has different practical meanings in different communities of experts. From a national security and defense perspective, it strongly overlaps with civil preparedness, with the difference that societal resilience stresses the broader range and diversity of actors who should come together to ensure a given level of resilience. This contrasts with the greater degree of centralization and of state control over critical infrastructure and critical functions of society that existed in NATO countries during the Cold War. As a result, in NATO discussions on societal resilience, it is common to stress the importance of public-private partnerships, of outreach to civil society, of empowering citizens, and of addressing international dependencies and vulnerabilities such as supply-chain vulnerabilities involving non-allies.

Building on these considerations, we offer the following definition of societal resilience in the context of national security and defense:

> The ability of a nation to draw upon all elements of society to resist, recover, learn, and adapt in the face of major shocks including armed attacks, to mitigate harm to the population, and to support the continuity of essential public services including security and national defense. Elements of society include individuals, civil society organizations, private enterprises, and public institutions. Beyond technical factors, societal resilience also hinges on intangible factors such as the extent of social bonds and social trust between individuals as well as between individuals and civil society, the private sector, and the public sector, thus enabling a combination of top-down and bottom-up responses. Other things equal, a more resilient society is one that suffers less harm from a first encounter with a given shock and adapts more ahead of a repeat occurrence and ideally also ahead of new types of shocks.

In practice, the enablement part of resilience remains largely in the hands of civilian public bodies and major corporations that can feasibly be subject to civilian or military authorities, as appropriate. However, we do not exclude enablement from our definition of societal resilience. In times of major crises, including war, bottom-up support from society can be materially useful and important for the morale of the armed forces and of the nation as a whole.

NATO's Baseline Requirements

In 2016, NATO members agreed resilience guidelines and pledged to achieve Baseline Requirements for National Resilience.[7] They further agreed a Strengthened Resilience Commitment in 2021. There are seven baseline requirements against which to measure their level of preparedness, which reflect the core functions of continuity of government, essential services to the population, and civil support to the military[8]. The

6 Caves et al., Enhancing Defense's Contribution to Societal Resilience in the UK, p. 8.

7 NATO, Warsaw Summit Communiqué, July 9, 2016, paragraph 73.

8 NATO, Resilience and civil preparedness – Article 3.

full description of the seven requirements and their supporting guidelines and evaluation criteria have not been publicly disclosed but are summarized on the NATO website as follows:

> **Assured continuity of government and critical government services**: for instance the ability to make decisions, communicate them and enforce them in a crisis;
> **Resilient energy supplies**: back-up plans and power grids, internally and across borders;
> **Ability to deal effectively with uncontrolled movement of people**, and to de-conflict these movements from NATO's military deployments;
> **Resilient food and water resources**: ensuring these supplies are safe from disruption or sabotage;
> **Ability to deal with mass casualties and disruptive health crises**: ensuring that civilian health systems can cope and that sufficient medical supplies are stocked and secure;
> **Resilient civil communications systems**: ensuring that telecommunications and cyber networks function even under crisis conditions, with sufficient back-up capacity. This requirement was updated in November 2019 by NATO Defence Ministers, who stressed the need for reliable communications systems including 5G, robust options to restore these systems, priority access to national authorities in times of crisis, and the thorough assessments of all risks to communications systems;
> **Resilient transport systems**: ensuring that NATO forces can move across Alliance territory rapidly and that civilian services can rely on transportation networks, even in a crisis.[9]

These baseline requirements share two characteristics: they are essential for a society under attack to continue to function and to mitigate civilian harm, and they are directly relevant to the continuity of military operations. (See Table 1.)

9 Ibid.

A more structured approach was endorsed by allies at the NATO summit in Madrid at the end of June 2022. Under this new approach, allies will be called upon to define national resilience goals and implementation plans, and to share these goals and plans with NATO staff and with each other through the alliance's newly established Resilience Committee. According to NATO officials consulted during the drafting of this paper, NATO staff will then produce a variety of assessments, most notably an alliance-wide strategic resilience assessment every four years. That assessment will in turn provide the NATO military authorities with a clearer picture of the alliance's resilience. Producing national resilience goals and implementation plans will be voluntary, but it is expected that a strong majority of allies will choose to do so from the start, with others likely following suit over time.

Cybersecurity as Crosscutting Priority

Cybersecurity is not identified as a separate function with its own NATO baseline requirement, owing to its crosscutting nature: it is critical for maintaining resilience across most, if not all, identified functions. Cyberattacks on government websites, banks, utilities, energy pipelines, media outlets, and water and sanitation facilities can cripple societies. They can prevent the effective functioning of government and cause widespread confusion, economic harm, and civil disorder. Cyberattacks on energy infrastructure, hospitals, and water services can lead to illness and the loss of life, putting them on par with kinetic means of warfare.

The coronavirus pandemic has increased the vulnerability of societies to cyberattacks. The advent of remote-work and an increase in digital government services[10] have pushed more activities online and increased the attack surface adversaries can exploit. At the same time, the intensity of attacks from malign state and non-state actors has grown since the beginning of the pandemic. While much of this activity is

10 United Nations, COVID-19 pushes more government activities online despite persisting digital divide, 2020.

Table 1. Military Implications of NATO's Baseline Requirements for National Resilience

Baseline Requirement	Military Perspective
Continuity of government	Continuity of civilian and democratic control of the armed forces Ability to communicate with and convey instructions to the civilian population Ability to collaborate with civilian government authorities First responders, and other services
Resilient energy supplies	Availability of fuel and grid electricity for military operations and command-and-control
Movements of people	Deconfliction with troop deployments and operational activities
Food and water resources	Provide for the nutritional needs of military forces Avoid limitations on military options due to a food crisis in the population
Ability to deal with mass casualties	Ensure civilian health services can support military requirements, and vice versa when appropriate, to treat injured personnel and to ensure sufficient supplies of medical and pharmaceutical products and equipment
Civil communications systems	Maintain the ability to use civilian communications infrastructure for operational needs, as appropriate, and to communicate to the population when necessary
Transport systems	Ensure that the civilian and commercial transport sector is available to support national priorities, including those of the armed forces, notably through provisions for the requisitioning of national and foreign-owned transport resources and for the establishment of prioritized transport corridors

commercial cybercrime, NATO need to be especially concerned about significant activity from state actors.

According to Microsoft, cyberattacks by state actors between July 2020 and June 2021 were primarily focused on intelligence collection, but in some cases were destructive, as with the attacks between Israel and Iran. In this period, 58 percent of attacks originated from Russia. The United States was the most targeted country, followed by Ukraine with 18 percent of attacks. This can now be seen in the context of Russia's invasion of Ukraine in February 2022.[11] These cyberattacks served as training for Russia's war. For example, in 2021, the Russian military group Sandworm took out power to 200,000 Ukrainian households, and in April 2022 launched cyberattacks at electric substations in Ukraine.[12]

11 Microsoft, Microsoft Digital Defense Report, October 2021.

12 Joe Tidy, "Ukrainian power grid 'lucky' to withstand Russian cyber-attack," BBC News, April 12, 2022.

Cyberattacks by states on critical infrastructure are a major concern, for this is where the potential for cyberattacks to become equivalent to kinetic attacks is most significant. In 2021, Microsoft found that China-based actors were more interested in targeting critical infrastructure than those based in Russia, North Korea, or Iran. Overall, 4 percent of attacks originating from states targeted critical infrastructure.[13]

The linkages between societal resilience and cybersecurity are only going to grow closer.

The linkages between societal resilience and cybersecurity are only going to grow closer. The increasing pace of digitalization and the rollout of the Internet of Things will lead to critical aspects of governance, communications, and critical services from medicine to border control being dependent on digital technologies. NATO members will have to closely monitor and improve their cybersecurity, with industry and civil society as close partners, to improve resilience across critical functions.[14]

The EU Directive on Critical Entities Resilience

For the 21 NATO members that are also members of the European Union, societal resilience will be shaped not only by the alliance's policies but also by policies pursued at the EU level. It is useful for allies outside of the EU to be aware of these developments, if only for awareness of what may drive EU allies to cohere around certain positions, but ideally also as a means of having some indirect access to useful reflections and additional best practice examples.

In December 2020, the European Commission adopted a proposal for a Directive on critical entities resilience (CER).[15] Cybersecurity is to be treated separately through the new Network and Information Systems Directive (NIS 2) Directive, which was proposed at the same time.[16]

The proposed CER Directive lays down harmonized minimum rules to enhance the resilience of critical entities. Ten sectors should be covered: energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, and space.[17]

Under the CER Directive, national authorities should produce a list of essential services (that is, those "essential for the maintenance of vital societal functions or economic activities") and, at least every four years, a risk assessment addressing "all relevant natural and man-made risks including (…) antagonistic threats". Member states should also identify all critical entities, namely those in the ten sectors that provide essential services and for which an incident would have significant disruptive effects. On that basis, member states should adopt national strategies for the resilience of their critical entities, to be updated at least every four years, covering at least the ten sectors identified, and setting out relevant objectives and governance and policy mechanisms to achieve those objectives.

The critical entities identified in each member state will in turn have to carry out their own risk assessments and to develop and implement resilience plans, with a view to managing risks, ensuring business continuity, and notifying incidents to competent authorities. Additional oversight measures will apply to critical entities that are of EU-wide significance, defined as ones that provides "essential services to or in more than one third of Member States".

Under the directive, the European Commission will chair a new Critical Entities Resilience

13 Microsoft, [Microsoft Digital Defense Report].

14 Additional thoughts on how NATO should approach cybersecurity can be found in another brief in this series: Merle Maigre, [NATO's Role in Global Cyber Security], The German Marshall Fund of the United States, April 6, 2022.

15 European Commission, Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities, [COM(2020) 829 final], December 16, 2020.

16 Ibid.

17 Ibid, Annex.

Group composed of its representatives and those of the member states. This group will among other tasks evaluate the national resilience strategies and examine national summary reports of incidents involving critical entities.

It is likely that many amendments to the directive will be requested by the European Council as well as by the European Parliament until an agreement is reached between them and with the European Commission. In its position adopted in December 2021, the European Council proposed to drop public administration as one of the ten sectors and also to rule out from the scope of the directive "any entity, either public or private, that mainly carries out activities in the areas of defense, national security, public security or law enforcement."[18] Should these changes be adopted, the CER Directive will entirely leave out the function referred to in the NATO context as continuity of government.

The CER Directive spells out legally binding requirements on national authorities in a manner that NATO's approach to resilience does not.

The CER Directive spells out legally binding requirements on national authorities in a manner that NATO's approach to resilience does not. However, NATO's progression toward national resilience goals and implementation plans, and their sharing and review collectively and with NATO staff, dovetails with similar objectives under the directive, in particular the obligation to produce national strategies setting out objectives and policy measures to enhance resilience. The perspectives pursued under EU and NATO auspices will retain key differences. For one thing, the EU approach does not include an explicit orientation toward enablement for the armed forces and will likely not address continuity-of-government issues. However, as noted, several key functions of society will be addressed at the EU and NATO levels, and at both EU alliance members will be developing national strategies and plans that identify objectives and policy measures to enhance resilience. There is therefore a positive opportunity for these countries to ensure in their national efforts a high degree of coherence between what they report through EU and NATO mechanisms.

The CER Directive mandates national authorities to consider "all relevant natural and man-made risks including (…) antagonistic threats." While the terms war or warfare are not used anywhere, EU members may include various scenarios of armed attack on their national territories or on those of other members as part of their risk assessments and as part of their national resilience strategies. Given the current international security environment, every member state should be encouraged to do so. However, significant disparities in national perspectives could emerge on this issue. In that case, the European Commission should encourage all member states to take adequate account of such scenarios, leveraging its agenda-setting role in the future Critical Entities Resilience Group. Relatedly, the group's European Commission chairperson and their NATO counterparts should liaise on a regular basis and to allow for regular briefings by NATO officials to the Critical Entities Resilience Group and by EU officials to NATO's Resilience Committee and to relevant NATO bodies. In parallel, EU alliance members should be encouraged to consider the same set of threats in NATO and EU consultations. An additional channel to promote coherence could be the meetings of the national senior officials for resilience that the allies agreed to designate in 2021 as part of the NATO 2030 agenda.[19]

18 Council of the European Union, Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities – General Approach, December 7, 2020, p. 17

19 NATO, NATO 2030, June 2021.

Advancing NATO's Work on Societal Resilience

NATO should see the developments at the EU level partly as a challenge but mainly as an opportunity. The challenge is that the implementation of the CER Directive will draw national authorities of EU alliance members into more discussions in the EU framework, potentially reducing the relative impact of NATO consultations in co-defining best practices for civilian perspectives on the sectors that are of interest at the EU and NATO levels alike. In order to maximize the value of both processes, NATO staff should develop a good awareness of EU-level discussions, especially those of the Critical Entities Resilience Group. With such an effort made, it may become easier to define the added value that NATO can bring to EU alliance members in particular, in civil preparedness as traditionally addressed and in the more expansive field of societal resilience.

It is important to evaluate the scope and effectiveness of NATO's baseline requirements relative to foreseeable needs, and the extent to which they sufficiently structure national efforts.

A first question is whether additional functions should be added to the seven baseline requirements. Differences in coverage emerge when comparing them with the ten sectors proposed by the European Commission. Wastewater is listed in the proposed CER Directive but it is not a distinct function for NATO. Wastewater ought to be addressed together with food and water resources: disruptions to its management can affect the availability of potable water for civilian and military needs. Furthermore, military installations have their own wastewater-treatment needs. Wastewater is a topic that should be of greater interest at the EU and NATO levels. The proposed directive also lists banking and financial market infrastructure, which are not addressed by NATO's baseline requirements. Armed forces continuously require, even in major combat operations, the ability to make and receive payments. Therefore, NATO should consider a new baseline requirement aiming at resilient payment systems.

Psychological defense also requires greater consideration. This relates to a long-established dimension of warfare—the morale of the civilian population, its will to fight to defend the country or to volunteer in other ways, and its resilience to enemy disinformation and propaganda. The example of Sweden is of particular interest in this field, given that it has a distinct government body, the Psychological Defense Agency (Myndigheten för Psykologiskt Försvar–MPF) that dedicated to these issues. The MPF aims to "strengthen the population's ability to detect and resist [foreign] malign influence campaigns and disinformation (…) [thereby contributing] to creating resilience and a willingness to defend the country."[20] In some respects, the MPF's activities will sound familiar to those engaged in, for example, debunking Russian disinformation, but they are broader on two counts. First, the agency works preventively and operationally, and second it fulfills its tasks in peacetime and in the event of war.

As the case of Ukraine illustrates, the stakes go beyond continuity of government—it is a matter of national continuity.

Psychological defense connects with the enablement of armed forces. These need to ensure the continued morale of their personnel, who may be exposed to hostile propaganda through a variety of channels. Ensuring education and awareness of the general public can lead to higher resilience among civilians and military personnel. Therefore, psychological defense should be discussed in the NATO context, perhaps beginning with an invitation to Sweden to provide expert briefings to relevant NATO committees.

The continued availability of essential digital data also merits more consideration. We propose to refer to this potential new area of work as "continuity of

20 Psychology Defense Agency, Our Mission, February 28, 2022.

data and infrastructure software."[21] States have long engaged in protecting sensitive information and seeking to acquire such data from potential adversaries, especially relating to defense and national security. However, digital data has become such an essential feature and resource of societies, economies, and governments that its loss or misuse is now potentially far more damaging. Ensuring the protection, integrity, and availability of data, and of the infrastructure software needed to make use of it, should thus be viewed as a critical national and societal function. A prospective baseline requirement would address protecting data resources and the ability to reconstitute them in case of loss or damage.

A specific goal would be secure cloud hosting, taking into consideration not only cyber threats but also kinetic threats against physical premises. Russia's aggression against Ukraine provides an important case study. Starting shortly before the war, Microsoft helped 16 of Ukraine's 17 government ministries as well as an unspecified number of Ukrainian companies move to the cloud.[22] As noted by the company's president, Brad Smith, Microsoft had

> not just to move their data and their infrastructure to the cloud, but to move it to the cloud outside Ukraine, and that's one of the most interesting lessons of this aspect of the work; the best way to protect a country in a time of war is to ensure its continuity by dispersing its digital assets […] governments are recognizing that you are most safe when people don't know where your data is.[23]

As the case of Ukraine illustrates, the stakes go beyond continuity of government—it is a matter of national continuity. The link to enablement is also clear. Armed forces may need to access civilian government or corporate data resources, and to be sure that enemy forces cannot access, corrupt, or destroy these.

Finally, there needs to be a sound approach to assessments of progress toward meeting the baseline requirements. Where relevant, a more codified approach, allowing for the generation of quantitative performance indicators, would be useful in eliciting a virtuous cycle of peer pressure among allies regarding which ones perform best. Summary quantitative indicators or indices could then be taken up either in "control panel" overviews of each ally's performance or in the form of country rankings, with a main focus on driving progress over time for each individual country.

Contributions from Finland and Sweden

NATO's approach to societal resilience is likely to become more robust thanks to the forthcoming memberships of Finland and Sweden. Facing a potentially hostile Soviet Union during the Cold War, the two countries developed whole-of-society approaches to defense. NATO can develop the most state-of-the-art approaches to this field by looking at their comprehensive policies. It can also benefit from their guidance not only on what level of resilience may be necessary but also, more importantly, on how to better consolidate aspects of societal resilience and on how to improve communication with and buy-in from citizens.

Sweden has a total defense concept to be carried out by military and civil defense. This approach was at its peak during the Cold War and declined after 1995. Russia's invasion of Crimea motivated Sweden to revive total defense in 2015.[24] The Defense Bill for 2021–2025 increases the civil defense budget and expands its scope. According to the government, "civil

21 We define infrastructure software as the essential software items that ensure the functioning of an organization. This includes items such as email, database servers, management software, and software that allows for data exchange with the organization's suppliers, clients, users, and other counterparts.

22 Zach Marzouk, "Microsoft says it's provided over $100 million in tech support to Ukrainian government", ITPro, May 20, 2022.

23 Alex Scroxton, "Nature of cyber war evolving in real time, says Microsoft president", Computer Weekly, May 19, 2022.

24 Regeringskansliet, Regeringen beslutar om återupptagen totalförsvarsplanering, December 10, 2015.

defense encompasses the whole of society and many actors must collaborate and work towards achieving its goal" and is carried out by government agencies, municipalities, regions, the business sector, and voluntary organizations.[25]

The functions covered by civil defense are similar to those on the NATO and EU lists but there are notable differences. In Sweden, 11 functions are listed: healthcare, food and drinking water supply, transport, law enforcement and security, financial preparedness, energy supply, electronic communications and mail, protective security, cybersecurity, protection of the civilian population, and psychological defense. The value of including psychological defense and financial preparedness (at least for payment systems) has been noted above. Contrary to the NATO approach, cyber-security is viewed as a function.

> ***NATO can learn from Finland and Sweden how to structure societal resilience in a manner that breaks down barriers between civilian and military actors across society and between agencies and authorities within the government.***

Finland labels its approach as comprehensive security, with a pragmatic and integrated vision at its core. According to the government, "Comprehensive security is the cooperation model of Finnish preparedness, where vital societal functions are handled together by authorities, businesses, NGOs and citizens."[26] These functions are leadership; international and EU activities; defense capability; internal security; economy, infrastructure, and security of supply; functional capacity of the population and services; and psychological resilience. Like Sweden, Finland prioritizes maintaining psychological resilience. But, unlike Sweden, NATO, and the EU, Finland lists fewer vital functions. The aim of this approach is to encourage crosscutting collaboration, interdependence, and communication.[27]

NATO can learn from Finland and Sweden how to structure societal resilience in a manner that breaks down barriers between civilian and military actors across society and between agencies and authorities within the government. The trust and sense of common responsibility this creates would reinforce the overall aims of societal resilience.

A second important lesson from the two countries is about the importance of citizen engagement and agency in defense. A key element of Sweden's total defense is the responsibility of each citizen to the country and to themselves. Sweden has a "total defense duty" that stipulates that everyone "between 16 and 70 can be called up to assist in various ways in the event of the threat of war and actual war. This might involve driving different means of transport, working in the health and medical care sector, or in a primary school, or otherwise helping ensure that society functions as well as possible."[28] Moreover, self-sufficiency is expected of the residents to increase resilience in a crisis. The Civil Contingencies Agency asks citizens to be "self-sufficient for a few days, or for up to a week or more. The most important things you will need are food, drinking water, heat, and the ability to receive important information."[29]

Not only do the authorities in Sweden make high demands of stakeholders across the whole of society, they also communicate relevant expectations and guidelines directly to the public; for example, with the 2018 brochure *If Crisis or War Comes*.[30]

25 Government Offices of Sweden, Objectives for Swedish total defence 2021–2025 - Government bill 'Totalförsvaret 2021–2025', December 18, 2020.

26 The Security Committee, Comprehensive Security.

27 Vesa Valtonen and Minna Branders, "Tracing the Finnish Comprehensive Security Model," in in Sebastian Larsson and Mark Rhinard (Eds.), Nordic Societal Security: Convergence and Divergence, Routledge, 2020.

28 Swedish Civil Contingencies Agency, Total defence – all of us together.

29 Ibid.

30 Swedish Civil Contingencies Agency, If Crisis or War Comes, 2018.

Finland's approach also prioritizes the agency of citizens and makes the expectations of them clear. Its "72-hour concept" sets out what each household should have to survive for 72 hours without state assistance in case of a crisis.[31] The authorities also consult citizens in the development of security policies including through in-person formats known as Security Cafés.[32]

NATO members should learn from the Finnish and Swedish approaches to engaging with citizens through government communications and in-person interactions to prepare them to be more helpful, self-sufficient, and resilient. Finland and Sweden have mandatory service requirements that may not be acceptable for all allies, but voluntary contributions to defense may be worth considering so as to create a positive relationship between military and civilian domains. Certainly, prioritizing communication and valuing citizen agency is a lesson applicable across NATO. If Finland and Sweden join the alliance, their practices and approaches could be better socialized across it and their experience drawn on in a crisis. The two countries would also benefit from NATO membership in the field of resilience. Membership includes requirements to measure against that are consistent with collective-defense objectives, along with access to NATO's pools of experts and to its civil crisis-management structure.

Conclusion

Regarding the eventual implementation of the EU's CER Directive, each EU alliance member should be encouraged to give adequate consideration to scenarios of armed attack against its territory or of armed attack against a fellow EU member or NATO ally, allowing for risk assessments and other outputs inherent to the directive to be fit for purpose. Relatedly, there should be close liaison work and briefings between the NATO International Staff and the European Commission representative who will chair the Critical Entities Resilience Group.

Three new functions should be added to NATO's baseline requirements: payment systems, psychological defense, and continuity of data and infrastructure software. Each addresses an important aspect of societal resilience while being relevant from the perspective of defense enablement. There should be a greater use of quantitative indicators for measuring progress in fulfilling NATO's baseline requirements for each ally.

As NATO looks forward to the future membership of Finland and Sweden, existing allies should learn from their comprehensive defense and security approaches and from their efforts to increase societal resilience. NATO can draw particular lessons from their approaches to fostering interdependence and cooperation across government and across society, and from their efforts to communicate directly with citizens in a manner that prioritizes the resilience and capabilities of the whole population during a crisis.

31 The Finnish National Rescue Association, 72 Hours – Could you cope on your own?"

32 Valtonen and Branders, "Tracing the Finnish Comprehensive Security Model."

About the Author(s)

Edward Hunter Christie is a senior research Fellow with the Finnish Institute of International Affairs and a research associate of the Wilfried Martens Centre for European Studies. He was a NATO official from 2014 to 2020 in roles pertaining to defense economics, strategic foresight, and technology policy, ending his tenure as deputy head of the Innovation Unit.

Kristine Berzina is a senior fellow for security and defense policy at the German Marshall Fund of the United States. She is based in GMF's Washington office, where she leads the security and defense portfolio and focuses on US security cooperation with Europe, NATO, US-EU relations, and sub-threshold threats including disinformation and energy. Before taking on this role, Berzina worked on countering autocratic influence as head of GMF's Alliance for Securing Democracy's geopolitics team.

Acknowledgments

The authors wish to thank Hasit Thankey at NATO and Christian Fjäder at the Finnish Institute of International Affairs for comments on an earlier version of the text.

This brief is part of a project at the German Marshall Fund of the United States supported by the Norwegian Ministry of Foreign Affairs.

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of the Second World War, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

G | M | F

Ankara • Belgrade • Berlin • Brussels • Bucharest
Paris • Warsaw • Washington, DC

www.gmfus.org