NATO PARLIAMENTARY ASSEMBLY

COMMITTEE ON THE CIVIL DIMENSION OF SECURITY (CDS)

ENHANCING THE RESILIENCE OF ALLIED SOCIETIES THROUGH CIVIL PREPAREDNESS

Preliminary Draft General Report

Joëlle GARRIAUD-MAYLAM (France)
General Rapporteur

011 CDS 21 E | Original: French | 3 March 2021

Founded in 1955, the NATO Parliamentary Assembly acts as a consultative interparliamentary organisation which is institutionally separate from NATO. This working document only represents the views of the Rapporteur until it has been adopted by the Committee on the Civil Dimension of Security. It is based on information from publicly available sources or NATO PA meetings – which are all unclassified.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

I. INTRODUCTION 1

II. THE PARALLEL EVOLUTION OF THE SECURITY ENVIRONMENT AND RESILIENCE POLICIES 2
- A. CIVIL PREPAREDNESS AT THE HEART OF DEFENCE DOCTRINES DURING THE COLD WAR 2
- B. THE EVOLUTION AND CURTAILING OF RESILIENCE-BUILDING EFFORTS DURING THE 1990s 3
- C. RENEWED INTEREST IN RESILIENCE POLICIES BASED ON CIVIL PREPAREDNESS TO COUNTER THE MULTIPLICATION OF SOCIETAL RISKS 3

III. TOWARDS A WHOLE-OF-SOCIETY APPROACH TO SECURITY RISK PLANNING AND MANAGEMENT 4
- A. THE ROLE OF CIVILIAN ACTORS IN CRISIS PREPAREDNESS AND RESPONSE 4
- B. THE IMPORTANCE OF HAVING CIVILIAN ACTORS COORDINATE WITH EACH OTHER AND WITH THE ARMED FORCES IN PREPARING AND RESPONDING TO CRISES 6

IV. NATO'S ROLE IN RESILIENCE AND CIVIL PREPAREDNESS 7
- A. RESILIENCE AS A CRUCIAL ELEMENT OF ALLIED SECURITY SINCE NATO'S INCEPTION 7
- B. RECENT DEVELOPMENTS IN NATO'S APPROACH TO RESILIENCE AND THE CREATION OF BASELINE REQUIREMENTS 7
- C. NATO STRUCTURES AND EXERCISES FOR RESILIENCE-BUILDING 8
- D. THE IMPORTANCE OF COOPERATING WITH PARTNER COUNTRIES AND THE EUROPEAN UNION TO BUILD SHARED RESILIENCE 9

V. THREE CASE STUDIES OF MEMBER STATES AND PARTNER COUNTRIES 10
- A. ESTONIA: A LEADER IN CYBER THREAT RESILIENCE 10
- B. FINLAND: AN EXEMPLARY WHOLE-OF-SOCIETY APPROACH TO SECURITY 11
- C. JAPAN: AN EXAMPLE OF RESILIENCE TO NATURAL DISASTERS 11

VI. CONCLUSIONS AND RECOMMENDATIONS 12

BIBLIOGRAPHY 15

EXECUTIVE SUMMARY

For Allied societies, the COVID-19 pandemic has painfully demonstrated the importance of strengthening their preparedness and capacity to respond to crises. Faced with an increasingly complex security environment and the multiplication of military and non-military threats affecting all of our societies, it appears more vital than ever to consolidate our resilience through civil preparedness.

Despite substantial efforts by NATO and Allied countries over the past two decades, vulnerabilities persist in this area. This preliminary draft report therefore calls on the Alliance to develop a whole-of-society approach to resilience, through which all civilian and military actors would function with greater synergy. It notably suggests taking inspiration from the successes of several Member States and partner countries. Finally, it offers recommendations to strengthen the capacities of our societies to counter present and future risks.

I. INTRODUCTION

1. In 2020, the outbreak of the COVID-19 pandemic had repercussions in the areas of healthcare, politics, the economy, society and security. It was a painful reminder of the need for Allied governments and societies to strengthen their preparedness and capacity to respond to all types of crises, whether military threats, natural disasters or epidemiological risks. Many governments had already identified the outbreak of a pandemic as a potential risk, yet very few had made it a priority to prepare for such a threat. The response of Allied societies was therefore not sufficiently effective. There were several adverse factors at play: the population's counterproductive reflexes; communication from the authorities that was at times unreliable; a damaging lack of coordination between various civil society actors and the authorities; flagrant inadequacies in multilateral and international cooperation; and frequent disruptions in supply chains. These shortcomings, combined with the spread of disinformation by hostile actors, have tested the democratic foundations of Allied systems and institutions.

2. One of the major lessons to be drawn from the difficulties faced in responding to the pandemic is the need to adopt a whole-of-society approach to resilience. In order to counter the current health crisis as well as future shocks and challenges, civilian and military actors must work in synergy. These concerns are not new. Since the creation of the Alliance and during the Cold War, Allied countries have established or consolidated policies to build resilience through civil preparedness. These efforts were supported and funded by both individual states and NATO. However, the gradual dissolution of the Soviet threat meant that the importance of these concepts temporarily faded in the Alliance's security policies.

3. Allies now face an increasingly complex and diverse security environment. In this context, the notion of resilience through civil preparedness is once again central to concerns about defence and crisis response. Thus, at the Warsaw Summit in 2016, Allied Heads of State and Government adopted a *Commitment to Enhance Resilience*. In it, they declare that "resilience is an essential basis for credible deterrence and defence and effective fulfilment of the Alliance's core tasks". Thereby, NATO recognises that the Alliance's military capacity and actions now depend to a large extent on civil sector support, expertise and infrastructures. It also notes that the security threats it faces are no longer all of a military nature and tend to affect every aspect of Allied societies, requiring a combination of military and civilian responses.

4. Nonetheless, addressing the challenges posed by present and future threats requires an even more fundamental cultural shift within the Alliance. While remaining committed to strengthening their military capability (notably by devoting 2% of GDP to defence spending), member countries should give a more central role to civilian actors who contribute to our societies' resilience in the face of crises. The private sector, national and local authorities, and above all citizens themselves must be recognised as full players in Member States' security. The resilience of our Alliance depends both on a better preparedness of these various civilian actors for present and future risks, and on effective and in-depth cooperation between them and with the armed forces.

Source: Centre d'excellence sur la cooperation civilo-militaire (CIMIC)

5. The concepts of civil resilience and preparedness should be defined at this stage. The notion of **resilience** is defined by NATO as a society's ability to resist and recover easily and quickly from a major shock such as a

natural disaster, failure of critical infrastructure, or a hybrid or armed attack (OTAN, 2018). A resilient society is thus a less attractive target for malicious outside actors, which reduces its exposure to traditional and non-traditional attacks and therefore also its vulnerability. Such a society is also more likely to bounce back from a large-scale natural disaster. The development of this capacity supposes a coherent interaction and preparation of civil and military actors prior to crises.

6. NATO also states that **civil preparedness** "means that basic government functions can continue during emergencies or disasters, in peacetime or periods of crisis" (NATO, 2020). The concept includes civil protection on the one hand, i.e., civil resilience in the event of war or threat of war, and crisis preparedness on the other, defined here as a society's ability to prevent and manage a crisis in peacetime.

7. In recent years, an increasing number of states have emphasised the notion of whole-of-society resilience as an objective of their security and crisis management strategies. The development of resilience through civil preparedness notably constitutes a central aspect of so-called "**total defence**" policies. These are found in certain NATO Member States such as Estonia and Norway, in partner countries such as Finland, Israel, Sweden and Switzerland, and in other nations such as Singapore. Total defence describes a security approach involving all of society, under the democratic control of political authorities, and through an institutional collaboration between these authorities, the armed forces, civil administrations, the private sector and the public. It aims to deter a potential enemy by increasing the cost of an attack and reducing its chances of success.

II. THE PARALLEL EVOLUTION OF THE SECURITY ENVIRONMENT AND RESILIENCE POLICIES

A. CIVIL PREPAREDNESS AT THE HEART OF DEFENCE DOCTRINES DURING THE COLD WAR

8. During the Cold War, national authorities in Allied countries developed "civil defence" (or "civilian emergency planning") policies to increase the resilience of societies through civil preparedness. The main objective of these efforts was to strengthen the capacity of local authorities to cope with a crisis and that of citizens to provide for their own needs if government authorities were temporarily incapacitated.

9. The efforts materialised in various forms: the construction of atomic bomb shelters; the development of mass evacuation plans; the constitution of local civil protection groups; and the creation of specialised government agencies. They also involved setting up public education programmes, notably by showing information videos in schools and distributing brochures to the general public on the steps to take in the event of an emergency, as was massively done in Sweden, for example.

10. Civil preparedness efforts were not limited to Allied nations during the Cold War. They were also considered strategically important on the other side of the Iron Curtain. The Soviet Union thus frequently organised large-scale emergency preparedness plans for its population. These included compulsory training for the public, periodic drills and alerts, and the wide dissemination of information on the role of citizens in the event of a crisis.

B. THE EVOLUTION AND CURTAILING OF RESILIENCE-BUILDING EFFORTS DURING THE 1990S

11. The end of the Cold War and the disappearance of the Soviet threat meant that efforts to build resilience through civil preparedness were relaxed in the 1990s, both at national and NATO levels. The likelihood of a conventional military attack on the territory of NATO states was now perceived to be low. In addition, the proliferation of crises beyond its borders pushed NATO to focus on "out of area" operations.

12. As a result, investments in this area were drastically scaled back. This notably led to the gradual privatisation and outsourcing of military tasks and infrastructure. During the Cold War, state resilience-building efforts were facilitated by the fact that many civilian assets with a key role in crisis management were under state control and could thus be quickly mobilised for defence purposes if required. Starting in the 1990s, civilian resources vital for national resilience, such as energy infrastructure and transport networks, became largely operated by corporate actors. Thus, according to NATO, around 90% of the military transport needed for large-scale military operations is now carried out by the private sector. Likewise, on average more than 30% of satellite communications used for defence purposes is provided by the private sector (NATO, 2018).

13. The programmes for resilience-building through civil preparedness that outlasted the 1990s now have different objectives. The focus has shifted from strengthening a society's readiness to cope with a military attack to improving its ability to respond to natural disasters. In Norway, for example, the Cold War era total defence policy has been revised and recentred on peacetime crisis preparedness (Wither, 2020). This development has allowed for a more integrated approach to civil preparedness, based on the fact that evacuation, communication and survival plans are largely the same for military and non-military threats.

C. RENEWED INTEREST IN RESILIENCE POLICIES BASED ON CIVIL PREPAREDNESS TO COUNTER THE MULTIPLICATION OF SOCIETAL RISKS

14. The emergence of the non-conventional threat posed by international terrorism within NATO's borders, particularly since the attacks of 11 September 2001, has led to renewed interest in resilience-building policies based on civil preparedness. The terrorist challenge and the threat of proliferation of weapons of mass destruction have influenced preparedness strategies. The scope of the latter was thus broadened to respond to a wide variety of threats, including chemical, biological, radiological or nuclear (CBRN) weapons and attacks against critical infrastructure.

15. Since then, the growing complexity of the security environment facing Allies has reinforced this trend. Today, NATO must tackle a broad and expanding range of risks, from the possibility of a conventional interstate conflict to threats from non-state actors, and including dangers posed by natural disasters and the current COVID-19 pandemic. Since 2014, Russia's recourse to hybrid warfare, which aims to weaken a society by exploiting its vulnerabilities, has also prompted Allies to rethink their approach to resilience (Gjørv, 2020). Moreover, NATO is increasingly sensitive to the growing threat that climate change poses to the resilience of our societies by magnifying the risks that already exist (Oppenheimer, 2020; Hill & Martinez-Diaz, 2020). These various factors endanger key machinery in our societies' functioning: communication, transport and healthcare systems; food, water and energy supplies; and the continuity of public authorities.

16. Faced with these risks, over the past two decades Allies have, to a certain extent, grown aware of the need to bolster defence capabilities by developing societal resilience and civil preparedness. To this end, they have adopted concrete measures at national and NATO levels. Nevertheless, the current pandemic has exposed a vital need for more substantial efforts.

III. TOWARDS A WHOLE-OF-SOCIETY APPROACH TO SECURITY RISK PLANNING AND MANAGEMENT

A. THE ROLE OF CIVILIAN ACTORS IN CRISIS PREPAREDNESS AND RESPONSE

National and local authorities

17. National and local authorities are responsible for building societal resilience. First, they establish the legislative and institutional framework that underpins a crisis response. They develop emergency plans and early warning tools and create systems to coordinate amongst themselves. In addition, before a crisis erupts, parliaments prepare legislation that enables authorities to act in response to a threat. They also ensure that appropriate funding is allocated to key areas such as the protection of critical infrastructure and the upkeep of stocks of essential and emergency goods. In this regard, it is important to highlight the need for a greater participation of women in national and local authorities in order to incorporate their contributions and needs into resilience-building efforts.

18. Second, national and local authorities help other civilian actors build the capacity to cope with a crisis in case government continuity or communication cannot be ensured. In particular, the public must be informed in advance of what measures to take in such a situation. For example, in 2018 Norway's Directorate for Civil Protection sent all households a brochure with instructions on what to do if essential public services were temporarily interrupted in an emergency, ranging from military conflict to a natural disaster (Wither, 2020). In Lithuania, the Defence Ministry and the Fire Department jointly developed a Crisis Response Handbook in 2015 (Flanagan, Osburg, Binnendijk, Kepe, & Radin, 2019).

19. Finally, when a crisis strikes a country, it is up to the authorities to make decisions, communicate with the public, and take the necessary steps to resolve it. This applies to the executive branch, but also to the legislature, which must be able to function even in a crisis. At the start of the pandemic, Allied parliaments were forced to briefly interrupt their work. Nonetheless, they proved innovative and flexible enough to quickly adapt the parliamentary process to the new health context (Cartier, Richard, & Toulemonde, 2020). The lessons learned from this difficult period for parliamentary assemblies must be formalised to strengthen our democratic institutions' resilience to shocks. In addition, making, communicating and enforcing the necessary decisions in the event of a crisis also requires setting up effective processes based on data and evidence, and using transparent and strategic communication to gain public trust and support. The vital role of these two aspects in developing an effective whole-of-society response to a crisis was amply demonstrated during the COVID-19 pandemic, especially because of the accompanying proliferation of disinformation. The lesson to be drawn is that before a crisis erupts, cultivating people's trust in the authorities' actions and information is essential to combat disinformation and propaganda and build civil preparedness.

The private sector

20. The private sector is both a source of strength and vulnerability for national resilience. Private companies promote efficiency and innovation, two indispensable qualities in the face of a crisis. However, their decisions are based on the pursuit of profit rather than resilience, which makes them less resistant to disruption. This was demonstrated during the COVID-19 pandemic. On the one hand, pharmaceutical companies developed innovative coronavirus vaccines in record time, which should bring this crisis to an end. On the other hand, reduced transport and factory closures disrupted supply chains and caused hold-ups. At the start of the crisis, we witnessed the impact of this as Allied countries were unable to obtain masks and other personal protective equipment, largely

manufactured by Chinese companies (Bradsher, 2020). Allied and global food supply chains were also affected by this crisis.

21. To better cope with threats and shocks, the private sector must, first of all, be integrated into resilience-building efforts prior to crises, so as to maximise its potential contribution when required. The private sector plays a central role in supplying essential goods and in the operation of key infrastructure. The armed forces rely on this when carrying out their defence mission, as does society as a whole when tackling a crisis. The contingency plans in this sector must be improved through cooperation with other actors to enable it to cope with large-scale disasters or threats that could potentially have major impacts across society.

22. Second, companies must ensure that they are themselves resilient to crises, beyond their contribution to societal resilience. This is particularly the case regarding cyber threats, which can obstruct their operations. Indeed, the risks associated with inter-sector connectivity have been amplified by the increasingly central role of the internet and information technology (IT) in our societies' functioning. All economic sectors now depend on IT, as do the critical infrastructures that support them. Current debates among Allies over 5G security demonstrate the importance of such critical infrastructures on the resilience of Allied societies.

23. As they become increasingly complex, integrated and interdependent, our societies display growing vulnerabilities that malicious actors seek to exploit. A breakdown in one economic area can lead to cascading disruptions in other areas with serious consequences for the entire society concerned (Schaake, 2020). The NotPetya cyberattack of 2017, launched by Russian hackers, demonstrated this by crippling millions of computers around the world, roughly half of them in Ukraine. In that country, the attack caused significant disruption by wiping data from computers owned by banks, energy companies, senior officials and an airport (Perlroth, Scott, & Frenkel, 2017). That same year, the WannaCry virus shut down parts of the UK National Health Service (NHS) and affected other organisations around the world (BBC, 2017). In 2020, it was the turn of researchers and companies involved in the development and distribution of COVID-19 vaccines to be the target of cyberattacks, notably from Russia (Kuchler & Murphy, 2020; Sabbagh & Roth, 2020).

24. Third, it is necessary to better monitor and support the ability of companies to take part in a crisis response. The increase in direct foreign investment in strategic segments of the Allied private sector, especially by China in Europe since the 2008-2009 crisis, is a source of concern for member countries' resilience capacity. For example, Chinese groups have invested in the commercial port of Piraeus in Greece, and in airports including London Heathrow, Frankfurt Hahn, Tirana and Ljubljana. These investments even extend to the energy sector, for instance the Hinkley Point C nuclear power plant project in Somerset, UK (Le Corre, 2018). The growth in such investments in several Allied countries raises questions about their ability to control and use these infrastructures in the event of a serious crisis. Allied governments must therefore consult with the private sector to assess the vulnerabilities of the latter and to arrange for corrective measures and contingency plans.

The civilian population

25. The civilian population is arguably the most crucial and most often overlooked actor in resilience. It is the target and/or the main victim of the majority of risks facing Allied countries. However, if properly prepared, it is also the first line of defence against these same threats. The COVID-19 crisis exemplified this. The effectiveness of the coronavirus response depends primarily on citizens' acceptance and respect of the measures set out by authorities.

26. Thus, it is crucial to place citizens at the heart of resilience-building efforts. They must be trained to deal with a crisis from its inception to its resolution, even if authorities are unable to provide their usual support. Public authorities must promote essential knowledge and skills among the

population before a crisis erupts. For example, the aforementioned brochure distributed to Norway's population includes information on necessary food stocks, emergency communication lines and first aid training. Other countries have developed such brochures and it would be advisable for all Allies to follow these examples. Likewise, the education system must be involved in training all youth, both girls and boys, in crisis response. Among other aims, these efforts should seek to develop young people's capacity to detect disinformation that undermines the authorities' ability to react and to gain citizens' trust in an emergency. The challenges of disinformation during the COVID-19 pandemic have underscored this need.

27. Finally, it is crucial to nourish a will among the civilian population to protect and defend the democratic principles that underpin our Allied societies. Security shocks can lead to a questioning of these principles, to political polarisation and social tensions, as was the case during the pandemic. Therefore, by developing more inclusive communication strategies and by involving the education system, authorities must constantly reaffirm and strengthen ties between citizens and their democratic values and institutions.

B. THE IMPORTANCE OF COORDINATION AMONG CIVILIAN ACTORS AND WITH ARMED FORCES IN CRISIS PLANNING AND RESPONSE

28. The armed forces are, of course, still the primary guarantors of Allied territorial integrity, deterrence and defence. Nonetheless, as they face increasingly diverse risks and vulnerabilities and grow more dependent on the civilian sector, they must fully engage in a whole-of-society approach to security. Today, an effective response to a crisis is impossible without the combined and coordinated involvement of the military and civilian sectors.

29. The COVID-19 pandemic has shown the positive impact that increased cooperation between the civilian sector and the armed forces can have during a serious crisis, including of a non-military nature. The military support of civilian structures, particularly in providing medical and logistical assistance, was one of the few positive aspects of the pandemic response. In Germany, for instance, some 15,000 military personnel were involved in administering tests, tracing chains of infection and providing emergency medical equipment. Similarly, in the UK, around 3,000 soldiers were deployed in November 2020 to assist civilian authorities with testing and logistical needs. Given its success, this cooperation between multiple actors in the civilian and military sectors — from the army to the police, and including national and local authorities, research institutes, the private sector and civil society — in the response to a crisis of a non-military nature, should certainly be formalised and sustained in the future.

30. To ensure that these sectors cooperate effectively when a crisis occurs, the relations between military and civilian actors should be made official and put into practice beforehand. Concretely, this means organising exercises to assess the synergy and interaction between civilian and military actors in the event of a crisis. Certain Allied countries already undertake regular exercises for this purpose. For example, in recent years, Latvia has taken additional measures to better coordinate ministerial efforts for national defence and has frequently conducted exercises to test their effectiveness. Lithuania has also organised large-scale exercises involving civilian institutions and based on unconventional threat scenarios. In addition, since 2013 this country has organised an annual exercise, *Flaming Sword*, to prepare its armed forces and various public authorities to jointly face hybrid threats (Flanagan, Osburg, Binnendijk, Kepe, & Radin, 2019).

31. Despite these positive examples of integration and coordination between the civilian and military sectors ahead of crises, much remains to be done to improve such cross-sector cooperation for resilience-building within Allied countries. This requires implementing cooperation agreements, organising preparedness and response protocols and training, and holding more comprehensive exercises that involve civilian and military actors across all NATO countries. In particular, good

practices already developed by some Allied states and partner countries should be generalised, notably those of the three states elaborated upon in chapter V.

IV. NATO'S ROLE IN RESILIENCE AND CIVIL PREPAREDNESS

A. RESILIENCE AS A CRUCIAL ELEMENT OF ALLIED SECURITY SINCE NATO'S INCEPTION

32. Resilience and civil preparedness are not only ambitions but also obligations for Allies. Elements underpinning the notion of resilience can already be found in the North Atlantic Treaty. Article 3 of the Treaty states: "the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack". Member States therefore consider that resilience depends on the Alliance's military capacity, on the state of civil preparedness of each Allied country, and on the coordination and integration of these two factors. States that are well prepared to respond to any type of attack or crisis are in fact less likely to be attacked. In this sense, Article 5 on collective defence and Article 3 on resilience are closely related.

33. Although resilience-building and civil preparedness are national prerogatives, since its creation, NATO has developed capacities, knowledge, structures and partnerships in these areas that benefit all Allies. NATO also plays a crucial role in coordinating national efforts and establishing common goals and benchmarks on the subject. In doing so, it makes the actions of Member States more coherent and effective.

B. RECENT DEVELOPMENTS IN NATO'S APPROACH TO RESILIENCE AND THE CREATION OF BASELINE REQUIREMENTS

34. The need for resilience has gradually come to encompass more than solely a response to armed attacks as envisaged by the Treaty. On the one hand, natural disasters can seriously affect the functioning of Allied societies. On the other, new risks, such as hybrid threats or cyber attacks, while they may not reflect the scale of an armed attack, still present a threat to Allied security. For this reason, at the Warsaw Summit in 2016, NATO Heads of State and Government adopted a *Commitment to Enhance Resilience*. In this text, they note that resilience in the face of new military and non-military threats requires Allies to "maintain and protect critical civilian capabilities, alongside and in support of military capabilities, and to work across the whole of government and with the private sector", as well as to cooperate with other international organisations, in particular the European Union and partner countries.

35. During that summit, on the basis of an initial assessment of national resilience capabilities (conducted the same year), the Allies defined seven baseline requirements in this area. These are used to measure and guide national resilience-building efforts and thus, by extension, those of the entire Alliance. They concern:

1. An assured continuity of government and critical government services: for instance the ability to make decisions, communicate them and enforce them in a crisis;
2. Resilient energy supplies: back-up plans and power grids;
3. The ability to deal effectively with the uncontrolled movement of people;
4. Resilient food and water resources: ensuring these supplies are safe from disruption or sabotage;
5. The ability to deal with mass casualties: ensuring that civilian health systems can cope and that sufficient medical supplies are stocked and secure;

6. Resilient civil communications systems: ensuring that telecommunications and cyber networks function even under crisis conditions;
7. The functioning of 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 (NATO, 2018).

36. A second assessment of each Ally's resilience capability was carried out in 2018 on the basis of these baseline requirements. It showed that, while the level of resilience and civil preparedness is high within the Alliance, additional efforts are needed in certain areas, particularly in the face of terrorist and CBRN risks.

37. In 2019, NATO leaders underscored the need to strengthen the resilience of critical infrastructure and communication systems. To this end, Allied defence ministers updated the corresponding Requirement 6 by emphasising the need for a reliable 5G network and efficient options to restore it if need be. They also indicated that national authorities should be given priority access to these networks in times of crisis, and that the risks faced by these systems should be subject to regular in-depth assessments.

38. At their June 2020 meeting, Allied defence ministers agreed that the need to update the baseline requirements would be reassessed in 2021. This update will be based on a third assessment of their application at the national level, which was finalised in 2020. Similarly, in their report to the Secretary General, the group of experts on the NATO 2030 reflection process placed the resilience-building of NATO, its member countries and their societies more broadly at the heart of its analysis and recommendations. The upcoming leaders' summit, along with the NATO 2030 process, will provide an excellent opportunity to reflect on the first lessons of the COVID-19 pandemic for transatlantic security, and to better prepare the Alliance for future challenges (De Maio, 2020).

C. NATO STRUCTURES AND EXERCISES FOR RESILIENCE-BUILDING

39. NATO has developed structures through which it can fulfil its mission to coordinate and support Member States in the area of resilience through civil preparedness. Established in the 1950s, the Civil Emergency Planning Committee (CEPC) is the main advisory body for civil preparedness and reports directly to the North Atlantic Council. It coordinates the planning of Allied nations and provides them with expertise in various fields. At the request of an Allied country, it can also deploy advisory support teams to help the latter identify ways to improve its resilience, as well as rapid reaction teams to respond to crises.

40. The CEPC oversees several technical planning boards and committees which design common Allied procedures to counter crisis situations. They bring together national government and industry experts as well as military representatives. They draw up emergency plans in areas including civil protection, transport, industrial resources, communications, public health, food and water. Furthermore, in 2020 the CEPC set up a process to draw lessons from the pandemic, aiming to help national authorities improve their level of preparedness and resilience.

41. The CEPC also oversees the activities of the Euro-Atlantic Disaster Response Coordination Centre (EADRCC). In the event of a crisis, the EADRCC shares information and coordinates relief efforts and capabilities among Member States and partner countries, as well as in countries where NATO has a military presence. It currently plays a role — albeit a limited one — in managing assistance and relief efforts in response to the COVID-19 pandemic, notably to coordinate the transport and provision of medical equipment. This role in international disaster relief should be developed. The EADRCC also conducts annual exercises to strengthen the coordination and preparedness of national authorities.

42. Another initiative, the Science for Peace and Security (SPS) Programme, promotes dialogue and practical cooperation between Member States and partner countries in the area of resilience through activities based on research, technological innovation and scientific knowledge exchange. Furthermore, although they are not a constituent part of NATO, several Alliance-accredited centres of excellence provide NATO with expertise in fields related to resilience and civil preparedness. These include centres of excellence for civil-military cooperation, cooperative cyber defence, disaster crisis management and defence against terrorism.

43. NATO also conducts exercises that put into practice the cooperation and interaction between Allied civilian and military sectors. For example, in 2018, the *Trident Juncture* exercise took place in Norway with 31 participating countries. It allowed Norway to test its resilience in the context of its "total defence" approach, assess its society's preparedness and identify any remaining vulnerabilities. As part of this exercise, the largest organised by NATO since the end of the Cold War, Norwegian armed forces cooperated closely with the Directorate for Civil Protection. The scenario involved private transport companies, the media, political and economic representatives, and non-governmental and international organisations. It also called on different civil sector capacities essential to societal resilience, such as logistics, cyber defence, strategic communication and civilian protection. Similarly, the multinational *Defender-Europe 20* exercise, led by the United States and conducted between January and March 2020, tested two crucial aspects of resilience: civil-military cooperation and enablement (i.e., the ability "to put in place the arrangements and infrastructure required to move units, as rapidly as possible, to wherever needed"). This was done through a major force deployment across the Atlantic and on continental Europe (Thomas, Williams, & Dyakova, 2020).

D. THE IMPORTANCE OF COOPERATING WITH PARTNER COUNTRIES AND THE EUROPEAN UNION TO BUILD SHARED RESILIENCE

44. With the ever-increasing digitisation and integration of our societies, vulnerability is no longer a matter of geography. An event beyond NATO's borders can quickly turn into a security crisis for the Alliance, as demonstrated by the spread of the coronavirus in the first months of 2020. Thus, cooperating closely with its partners on resilience allows the Alliance to support them and increase the stability of its neighbourhood. Moreover, it is a way for NATO to strengthen its resilience by exchanging best practices with its partners, including in areas where Allies still have progress to make. This need was highlighted by the COVID-19 pandemic, which some countries responded to much more effectively, particularly in Asia and Oceania (e.g., Taiwan, New Zealand and Vietnam, among others) (The Economist, 2020).

45. NATO has developed in-depth relations with certain partner countries in the area of pre-crisis resilience. For instance, in February 2019 it deployed a team of civil preparedness experts to support Ukraine. NATO also launched a three-year joint project with the United Nations in 2019 to help Jordan improve its preparedness for the threat posed by CBRN weapons (UNOCT, 2019).

46. It also cooperates closely with Sweden and Finland to counter hybrid threats by organising consultations, training, and joint exercises (NATO, 2019). In addition, it actively contributes to crisis response in partner countries. During the pandemic, it has provided support to many partner states by distributing medical and food supplies. Likewise, in June 2020 the EADRCC coordinated the Allied response to severe flooding in Ukraine.

47. Building resilience is also a focus of cooperation and coordination efforts between NATO and the EU. In 2016, the two organisations adopted a joint declaration and joint proposals that explicitly refer to resilience-building. Their stated intentions are: to increase interaction between their staff in this area; to strengthen the coherence of their respective policies and plans; and to be prepared to deploy experts in a coordinated manner to help boost the resilience of Member States, either in the

pre-crisis phase or in response to a crisis. In recent years, NATO and the EU have transformed these commitments into concrete cooperation, particularly in the fields of cyber security and defence, and in the fight against hybrid threats.

V. THREE CASE STUDIES OF MEMBER STATES AND PARTNER COUNTRIES

A. ESTONIA: A LEADER IN CYBER THREAT RESILIENCE

48. The Baltic states must tackle the conventional threat posed by Russian armed forces close to their borders. They are particularly affected by Russian disinformation and propaganda campaigns, and face risks of hybrid attacks by Moscow. Estonia has had a bitter taste of the potential impact of these risks. In April and May 2007, the country was confronted with an unprecedented cyberattack, which the authorities claimed was launched from Russia. For three weeks, denial of service attacks impacted the websites of the country's government, news agencies, Internet service providers, large banks and small businesses. These attacks caused serious disruptions to Estonia's society at a cost of several billion euros (Tamkin, 2017). They have changed the country's approach to resilience and civil preparedness.

49. From 1993 to 2010, Estonia's concept of national security was based on the principles of total defence and territorial defence. Nevertheless, in response to the evolution of the security environment and in particular the 2007 attacks, the authorities updated their concept of national security and their national defence strategy, in 2010 and 2011 respectively. The two corresponding texts recognised that the threats facing the country no longer necessarily called for a largely military response as advocated by their predecessors. Rather, they recommended the integrated use of a wide range of military and non-military means.

50. In particular, after the 2007 attacks, the country's priority became the cyber-threat resilience of society as a whole. One of the main objectives of the Estonian cyber security strategy for 2019-2022 is thus to invest in "a sustainable digital society with strong technological resilience and crisis preparedness" (Ministère des d'économie et de la communication, 2019). The country has adopted a cross-sector approach to cyber governance and cyber defence, supported by a Cyber Security Council. An Information System Authority and a Cyber Command were created within the ministries of the economy and the armed forces respectively. Finally, Estonia hosts the NATO-accredited Cooperative Cyber Defence Center of Excellence and organises NATO's *Locked Shields* and *Crossed Swords* exercises (Kohler, 2020). Its efforts in the area of cyber resilience make Estonia an example for other Allies to follow.

51. Since 2014, Russia's illegal and illegitimate actions have contributed to Estonia's reassessment of its security policy. In 2017, the country once again updated its national security approach, now based on the concept of "integrated defence and total security". This incorporates the whole of society and includes six pillars: military defence; civilian support for military defence; international action; internal security; the continuity of the state and society; and psychological defence. The Estonian model gives every actor in society an important role to play. Risk management is highly decentralised but made effective by strong coordination between different sectors. In addition, Estonia benefits from the expertise of the Estonian Defence League, a voluntary national defence group, organised militarily and under the command of defence forces. Its 16,000 members support the Estonian armed forces in various tasks. They also train the population in national defence and resilience. Annual exercises are organised to test the resilience and coordination capabilities of all civilian and military actors. In particular, the *Siil* exercise tests the army's ability to cooperate with the police, border guards, the relief council and the Defence League (Flanagan, Osburg, Binnendijk, Kepe, & Radin, 2019).

B. FINLAND: AN EXEMPLARY WHOLE-OF-SOCIETY APPROACH TO SECURITY

52. Finland is a non-aligned country with a long land border that it shared with the Soviet Union, which it fought in 1939-1940 to maintain its independence. During the Cold War, the country adopted a total defence doctrine, largely based on civil preparedness and deterrence through resilience (Wither, 2020). Unlike some of its neighbours, when the Cold War ended Finland continued to mobilise the whole of society as part of its total defence efforts. The country's latest "Security Strategy for Society", adopted in 2017, aims to preserve the vital functions of society in the event of a crisis, and gives clear directives to each sector of society on how it should prepare for and respond to potential risks. It is implemented through specific strategies for certain administrative branches, as well as cross-sector and thematic strategies, including one on cyber security.

53. Finland's Security Strategy for Society is "based on the principle of comprehensive security in which the vital functions of society are jointly safeguarded by the authorities, business operators, organisations and citizens" (Comité de sécurité, 2017). The armed forces are, of course, central to the concept of comprehensive security, notably through a compulsory national service. Nevertheless, the whole of society is involved in the country's security (Salonius-Pasternak, 2018). This comprehensive security plan is prepared and put into practice by the Security Committee, which coordinates the actions of the ministries and assists the government in this area. The Committee is made up of around 20 senior officials and experts from national authorities and, it is worth noting, the private sector.

54. The strategy places particular emphasis on "psychological resilience", which it defines as "the ability of individuals, communities, society and the nation to withstand the pressures arising from crisis situations and to recover from their impacts". In the event of a crisis, psychological resilience is seen as a critical factor in maintaining the will of the Finnish people to defend their country (Comité de sécurité, 2017). Its role is crucial in thwarting propaganda and disinformation campaigns which, according to a 2018 assessment by Finnish authorities, represent a major risk to the country's resilience, along with terrorist attacks and upheavals caused by climate change.

55. This same assessment identified other risks that could affect society's stability, including a serious disruption of the economy, a military attack and large-scale immigration (Ministère de l'intérieur, 2018). To counter these various man-made and natural risks that challenge the resilience of its society, Finland has developed an international cooperation strategy. It notably cooperates with NATO and the EU, and hosts the European Centre of Excellence for Countering Hybrid Threats, affiliated to the two organisations. On a national level, it has acquired significant expertise in planning, leading exercises and developing resources. The country stocks food, fuel, fodder, and equipment for civil defence and, according to official figures, has 45,000 civil defence shelters that can accommodate 3.6 million citizens.

C. JAPAN: AN EXAMPLE OF RESILIENCE TO NATURAL DISASTERS

56. Japan provides an example of resilience to natural disasters on a global scale. Japanese society is regularly struck by earthquakes, tsunamis and floods, and has had to learn to live with these risks. Notably, on 11 March 2011, an earthquake in the Pacific off the coast of Tōhoku region triggered a tsunami that caused an accident at the Fukushima Daiichi nuclear power plant. This natural disaster killed nearly 20,000 people, injured around 6,000 and required the evacuation and displacement of approximately 470,000 citizens (Japanese reconstruction agency, 2021). The resulting economic losses were estimated at roughly $210 billion (OECD, 2019). In view of these figures and the high probability (estimated at 70-80%) of a major earthquake in the next three decades (OCDE, 2019), national resilience-building in the face of natural disasters is a priority for Japan.

57. Following the disaster of 2011, Japan further developed its already advanced capabilities and knowledge in the areas of risk anticipation and resilience through civil preparedness. The country learned crucial lessons from the 2011 disaster and its aftermath. These lessons were incorporated into a Basic Act for National Resilience passed in 2013, which resulted in a Fundamental Plan for National Resilience (adopted in 2014 and updated in 2018) and an action plan (Bureau de la promotion de la résilience nationale, 2015). The Fundamental Plan is structured around four main axes: 1) preventing human losses by all possible means; 2) avoiding the failure of the administration and of social and economic systems; 3) minimising damage to property and facilities; and 4) enabling rapid reconstruction after a natural disaster.

58. In addition, the Japanese approach to resilience is upheld by several guiding principles. First, it is based on the principle of subsidiarity. All local authorities must develop a fundamental resilience plan for their own jurisdictions (OCDE, 2019). Crisis anticipation and management is thus largely delegated to local authorities. The Cabinet Office nevertheless provides oversight and coordinates these efforts. If decision-making structures and local communication channels break down, as was the case in certain municipalities in 2011, the government can also quickly regain control of the response management.

59. Second, the Japanese strategy in this area relies on close cooperation between the authorities and the private sector. The latter is encouraged to contribute to civil preparedness and resilience through education and training programmes on how to respond to natural disasters. In addition, the use of private capabilities and equipment in times of crisis is explicitly encouraged by the Fundamental Plan for National Resilience.

60. Third, Japan's resilience policy relies on strong cooperation between the civilian sector and Japanese self-defence forces. Prior to crises, the armed forces are consulted in the development of fundamental plans and improve their coordination with local authorities through regular exercises. In the event of a major crisis, the armed forces are thus able to react quickly and efficiently to support national and local authorities. To ensure effective communication between these various bodies, retired army officers work in prefectures and municipalities across the country (Wambach, 2012).

61. Finally, Japan's strong resilience to natural disasters is the result of advanced civil preparedness efforts. Drills for earthquakes and other natural disasters are regularly organised in schools across the country. The knowledge and skills acquired through such training in emergency procedures helped save many lives during the 2011 disaster (Wambach, 2012).

VI. CONCLUSIONS AND RECOMMENDATIONS

62. Today's security environment is characterised by an increase in military and non-military threats that impact all of our societies. They notably affect the civilian sector, and especially the population. The Alliance must therefore adopt a whole-of-society approach to resilience, in which all civilian and military actors work in synergy and can respond effectively to crises of every nature. Although Allied countries and NATO largely lost interest in resilience and civil preparedness policies following the end of the Cold War, over the past two decades they have made substantial efforts in these areas. Nevertheless, much remains to be done to strengthen the capacity of the Alliance and our societies to counter present and future risks. To this end, it would be advisable to:

1. ***Adopt the means to match our ambitions:*** Resilience-building requires investment. To achieve the objectives that Allies have set themselves in terms of building societal resilience, member countries and NATO must provide sufficient financial and human resources on top of the commitment to devote 2% of GDP to defence spending.

2. ***Identify vulnerabilities and assess capabilities:*** Member States should undertake regular, critical assessments of their vulnerabilities and capabilities, both individually and collectively. To facilitate this process, NATO must develop more easily measurable requirements and guidelines that allow Allies to quantify and compare their progress.

3. ***Support the exchange of best practices***: While respecting national specificities and responsibilities, it is crucial to better share the lessons learned and the expertise developed by certain Member States and partner countries in specific areas, for example: Estonia on cyber threats; Finland on establishing a whole-of-society approach to resilience; and Japan on anticipating and responding to natural disasters. These practices could be replicated in other Allied and partner countries following more in-depth exchanges between them.

4. ***Adopt a more comprehensive and integrated approach to crisis planning and management****:* Faced with a broad and expanding range of risks that call for both military and non-military responses, it seems necessary to strengthen pre-crisis cooperation between the armed forces on the one hand, and national and local authorities, the private sector and the population on the other. This cooperation should include the design of early warning systems and emergency plans that can guarantee a rapid and effective response in the event of a crisis.

5. ***Test our capacities in order to improve them:*** Additional exercises must be organised, both at a national and NATO level, to put into practice, test and improve emergency plans prior to crises. They should:

    a. Include all sectors of society and consider their growing interdependence as well as the negative impact and risk of a chain reaction that the failure of one actor can have on others.
    b. Be based on scenarios that take into account both traditional threats, such as armed conflict, and non-military risks like natural disasters and pandemics, as well as hybrid threats (disinformation, cyberattacks, etc.).
    c. Test our systems to breaking point so that various civilian and military actors can identify and mitigate their own vulnerabilities.

6. ***Enhance communication and education initiatives aimed at the civilian sector and the public to underscore the importance and benefits of resilience in order to create a resilient mindset:*** Building the resilience of Allied societies requires the participation and cooperation of all civilian and military actors. Member States and NATO must therefore develop shared and active awareness-raising policies, aimed at citizens and actors of the civilian and military sectors, on the need for and value of resilience. Allies should also educate their citizens about resilience in schools and universities.

7. ***Develop planning initiatives within the private sector:*** The COVID-19 pandemic has shown how vital it is for the private sector, in cooperation with armed forces and authorities, to better anticipate and prepare for crises by developing strategies to:

    a. Guarantee that contingency plans exist and can be activated to maintain services essential to the population or to the armed forces as part of their crisis response;
    b. Limit unnecessary interconnections between critical infrastructures and in supply chains, and ensure that necessary ones are identified and replaceable to minimise the risk of cascading disruptions in the event of a crisis.

8. ***Implement and improve foreign investment assessment mechanisms:*** Such tools are needed to ensure that critical infrastructures can serve the national security and defence of Allied countries and their armed forces in the event of a crisis.

9. ***Strengthen the democratic resilience of our societies:*** The values and principles on which our democracies are founded have, to a certain degree, been challenged by the COVID-19 pandemic. In order to ensure our societies' ability to better anticipate, prepare for and respond to crises, it is essential to reaffirm the democratic principles at their core, and to improve the way these are concretely implemented. To do so, as suggested by the President of the NATO Parliamentary Assembly, Gerry Connolly, a Centre for Democratic Resilience should be created within NATO, with the role of supporting Allied countries in strengthening their democratic systems and institutions. This Centre would conduct research and provide advice and assistance to Member States in areas including electoral integrity and security, judicial independence, freedom of the press, and the fight against disinformation (Connolly, 2019; NATO 2030 Reflection Group, 2020).

10. ***Increase the participation of women and better integrate gender issue in resilience policies:*** As the pandemic response once again demonstrated, women play a crucial role in our societies' resilience. It is therefore essential to increase their participation in the political bodies and security institutions responsible for anticipating, preparing for and responding to crises. In addition, the question of gender should be better integrated into every phase of crisis management. The specific needs and contributions of women must be taken into account in crisis planning and response, and in post-crisis rehabilitation and reconstruction.

11. ***Enhance cooperation between NATO and the EU:*** Stronger cooperation should enable both organisations to better identify common threats and vulnerabilities and share best practices. Moreover, they should work together to distinguish between areas where their resilience-building efforts overlap, and those where further cooperation could bring added value. The skills and capacities of the two organisations could thus be deployed more rationally and effectively.

12. ***Develop existing partnerships and create new ones***: Allies should build ties with partner countries that have acquired knowledge and capacities in generating resilience to various types of potential crises. It would also be advisable to strengthen relations with other states with which no formal partnerships exist, but from which Allies have much to learn. These include certain countries in Asia and Oceania that have displayed an exceptional capacity for resilience during the COVID-19 crisis.

13. ***Draw lessons from the COVID-19 pandemic and prepare for future crises resulting from climate change:*** The CEPC has established a process that allows it to draw lessons from the pandemic in the fields of civil preparedness and resilience. It should be able to identify the best practices implemented at national levels and share these with other Member States and partners. This process deserves to be maintained, institutionalised and extended beyond the pandemic. It could thus serve as a forum to exchange ideas and best practices concerning NATO's planning and management of non-military threats such as pandemics, but also climate change. In this manner, the response to future crises could be better coordinated and more effective.

14. ***Place resilience at the heart of the reflection on the Alliance's future:*** Strengthening the resilience of Allied societies through civil preparedness is one of the themes most extensively addressed in the report by the group of experts from the NATO 2030 reflection process. This topic should be a focus of discussions between Allied Heads of State and Government on the future of the Alliance, as well as within the NATO Parliamentary Assembly.

BIBLIOGRAPHY

BBC. (2017). *bbc.com*. www.bbc.com/news/technology-41753022

Bradsher, K. (2020). *nytimes.com*. www.nytimes.com/2020/07/05/business/china-medical-supplies.html.

Japanese National Resilience Promotion Office. (2015). *cas.go.jp*. www.cas.go.jp/jp/seisaku/kokudo_kyoujinka/en/e01_panf.pdf

Cartier, E., Richard, B., & Toulemonde, G. (2020). Fondation Robert Schuman: https://www.robert-schuman.eu/en/doc/ouvrages/FRS_Parliament.pdf

Connolly, G. (2019). *nato-pa.int*. www.nato-pa.int/download-file?filename=%2Fsites%2Fdefault%2Ffiles%2F2019-11%2FRAPPORT%20146%20PCTR%2019%20F%20rev.%201%20fin%20-%2070%20ANS%20DE%20L%27OTAN%20-%20POURQUOI%20L%E2%80%99ALLIANCE%20DEMEURE%20T%20ELLE%20INDISPENSABLE.pdf

De Maio, G. (2020). *brookings.edu*. www.brookings.edu/research/natos-response-to-covid-19-lessons-for-resilience-and-readiness/

Estonia, Ministry of economic affairs and communications. (2019). *Cybersecurity Strategy*. *mkm.ee*. www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Finland, Security Committee (2017). Security strategy for society turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf

Finland, Ministry of the Interior (2018). *ec.europa.eu*. ec.europa.eu/echo/sites/echo-site/files/national_risk_assessment_2018.pdf

Flanagan, S. J., Osburg, J., Binnendijk, A., Kepe, M., & Radin, A. (2019). *rand.org*. www.rand.org/pubs/research_reports/RR2779.html.

Gjørv, G. H. (2020). *nato.int*. www.nato.int/docu/review/articles/2020/05/20/coronavirus-invisible-threats-and-preparing-for-resilience/index.html

Hill, ., & Martinez-Diaz, L. (2020). *foreignaffairs.com*. reader.foreignaffairs.com/2020/01/23/adapt-or-perish-2/content.html

Kohler, K. (2020). *css.ethz.ch*. css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Estonia.pdf

Kuchler, H., & Murphy, H. (2020). *ft.com*. https://www.ft.com/content/9c303207-8f4a-42b7-b0e4-cf421f036b2f?accessToken=zwAAAXZq78xIkdOcMDIHj0pCt9Ow5M9CHwNrLw.MEUCIDt9595iGse_C05tTG8J4tl3wZSRGn9Gzm6vaMHOUHaWAiEA6lYx-kThkt6OwU9IvKJBjvBjVgfQWxXFWX5MskMMtHU&sharetype=gift?token=59e3ba00-e807-41ea-9bb9

Japanese reconstruction agency (2021). www.reconstruction.go.jp/english/topics/GEJE/

Le Corre, P. (2018). Experiences and Lessons for the “Belt and Road” Initiative carnegieendowment.org/files/RethinkingtheSilkRoad.pdf

NATO. (2018). *Resilience and Article 3,* https://www.nato.int/cps/en/natohq/topics_132722.htm?selectedLocale=en

NATO. (2019). *nato.int*. www.nato.int/nato_static_fl2014/assets/pdf/2020/3/pdf_publications/sgar19-en.pdf

NATO. (2020). Civil preparedness, https://www.nato.int/cps/fr/natohq/topics_49158.htm?selectedLocale=en .

NATO 2030, Reflection Group. (2020). *nato.int*. www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

OECD. (2019). *oecd-ilibrary.org*. www.oecd-ilibrary.org/sites/9789264311602-8-en/index.html?itemId=/content/component/9789264311602-8-en

Oppenheimer, M. (2020). *foreignaffairs.com*. reader.foreignaffairs.com/2020/10/13/as-the-world-burns/content.html

Perlroth, N., Scott, M., & Frenkel, S. (2017). *nytimes.com*. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html

Sabbagh, D., & Roth, A. (2020). *theguardian.com*. www.theguardian.com/world/2020/jul/16/russian-state-sponsored-hackers-target-covid-19-vaccine-researchers?CMP=Share_AndroidApp_Outlook

Salonius-Pasternak, C. (2018). *fiia.fi*. www.fiia.fi/wp-content/uploads/2018/06/bp240_the-defence-of-finland-and-sweden.pdf

Schaake, M. (2020). *foreignaffairs.com*. https://reader.foreignaffairs.com/2020/10/13/the-lawless-realm/content.html

Tamkin, E. (2017). *foreignpolicy.com*. foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

The Economist. (2020). *economist.com*. www.economist.com/asia/2020/12/12/the-japanese-authorities-understood-covid-19-better-than-most?frsc=dg%7Ce%3cspan%20id=%22ms-outlook-android-cursor%22%3e!~OMSelectionMarkerEnd~

Thomas, G., Williams, P., & Dyakova, Y. (2020). *nato.int*. www.nato.int/docu/review/fr/articles/2020/06/16/exercice-defender-europe-20-la-facilitation-et-la-resilience-en-action/index.html

UNOCT. (2019). *un.org*. www.un.org/counterterrorism/events/unoct-and-nato-launch-project-prevent-and-counter-chemical-biological-radiological-and

Wambach, J. (2012). *reliefweb.int*. reliefweb.int/sites/reliefweb.int/files/resources/Liaison2012_Web.pdf

Wither, J. K. (2020). *tandfonline.com*. www.tandfonline.com/doi/full/10.1080/14702436.2020.1718498