Preparing Populations for Hybrid Threats against Critical Infrastructure: The European Experience

Author: Heather S. Gregg, PhD

This report was sponsored by the Irregular Warfare Center under contract HQ0034-24-C-0108

About the Author

Dr. Heather S. Gregg is a research fellow for the Future Security Initiative at Arizona State University and senior nonresident fellow at the Foreign Policy Research Institute.

Dr. Gregg's academic focus is on irregular warfare, hybrid threats, terrorism and counterterrorism, causes of extremism, and leveraging culture in population-centric conflicts, including building societal resilience and repairing communities and national unity in the wake of war and political instability.

Dr. Gregg has held several academic positions in the U.S. Department of Defense. She was professor of Irregular Warfare/ Hybrid Threats at the George C. Marshall European Center for Security Studies (2023–2024), professor of military strategy at the U.S. Army War College (2019–2022), and associate professor at the Naval Postgraduate School in Monterey, California, where she worked primarily with Special Operations Forces (2006–2019). She is the 2017 recipient of the NPS school-wide Hamming Award for excellence in teaching. Dr. Gregg was also an associate political scientist at the RAND Corporation (2003–2006). She has conducted research for the DoD, USASOC, USSOCOM, OSD, TRADOC, NCTC, JIEDDO, and DoS.

Dr. Gregg earned her PhD in Political Science in 2003 from the Massachusetts Institute of Technology. She also holds a master's degree from Harvard Divinity School, where she studied Islam, and a bachelor's degree in Cultural Anthropology, with honors, from the University of California, Santa Cruz.

Dr. Gregg has worked with allies and partners on a range of security issues. She has lectured for NATO courses, and for conferences and workshops on countering hybrid threats, building societal resilience, and countering violent extremism. From 2013–2015, she was part of teaching and engagement teams in Tajikistan. In 2016, she taught at the Indonesian Defense University on subjects relating to asymmetric warfare. Most recently, she has participated in a series of engagements with NATO's Center of Excellence, Defense Against Terrorism in Ankara, Türkiye, and the Irregular Warfare Center in the United States.

Dr. Gregg has published extensively on irregular warfare/hybrid threats, religiously motivated conflict, and extremism, including: "Hybrid Threats and Strategic Competition" (*Connections,* 2024); *Religious Terrorism* (Cambridge University Press, 2020); "Religiously Motivated Violence" (Oxford University Press, 2016); *Building the Nation: Missed Opportunities in Iraq and Afghanistan* (University of Nebraska, 2018); *The Path to Salvation: Religious Violence from the Crusades to Jihad* (University of Nebraska, 2014); and co-editor of *The Three Circles of War: Understanding the Dynamics of Modern War in Iraq* (Potomac, 2010).

Table of Content

Executive Summary

One of the most persistent security threats the United States (U.S.) faces today is a range of hostile activities short of open armed conflict. These activities occur in what is often called the "grey zone," which blurs the distinction between traditional war and peace and includes actions such as manipulating information, deploying hostile cyber activities, and working through proxy forces to achieve various effects.[1] These threats are sometimes difficult to detect and almost always difficult to clearly attribute to an actor, making a response challenging.

Our European allies and partners call these activities "hybrid threats."[2] When combined with kinetic operations, this is hybrid warfare.[3] U.S. Joint Doctrine 1 Vol. 1, "Joint Warfighting" (2023) refers to these, among other activities, as "irregular warfare," which it defines as "a form of warfare where state and non-state actors campaign to assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities, either as the primary approach or in concert with conventional warfare."[4]

The principal target of hybrid threats is people, what is sometimes called the "human domain."[5] Adversaries target populations with the hope that they will panic, overreact, and blame their governments for the inability to stop the attack. Ultimately, hybrid threats aim to sow fear and mistrust within societies and between citizens and their governments, challenging the government's legitimacy and preventing states from projecting power both internally and internationally.

Hybrid attacks on critical infrastructure (CI)—including energy grids, fuel pipelines, water and sewage systems, communications infrastructure, and banking and financial systems—are especially challenging for governments because they are difficult to prevent and not only affect a population's access to critical goods and services but can also diminish trust in the government's ability to protect CI and provide these lifegiving resources.

Preparing populations for disruptions to goods and services caused by hybrid attacks against CI, therefore, is important because the population's response is a critical part of the adversary's strategy, and preparing populations to withstand the effects of hybrid threats helps to undermine the adversary's plan.

This report investigates how hybrid threats against CI pose a particular vulnerability to countries today and how governments can prepare their populations for disruptions in goods and services due to these attacks. Specifically, it asks:

---

1 See, for example: "The Gray Zone," U.S. Special Operations Command, September 9, 2015. https://info.publicintelligence.net/USSOCOM-GrayZones.pdf.

2 Hybrid COE's definition describes hybrid threats as a "concept," which "refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution."; "Hybrid threats as a concept," Hybrid COE, accessed November 22, 2024, https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

3 Mikael Weissmann, "Conceptualizing and Countering Hybrid Threats and Hybrid Warfare," in *Hybrid Warfare: Security and Asymmetric Conflicts in International Relations*, ed. Mickael Weissmann et al. (I.B. Tarus, 2021), 65-66.

4 "Joint Doctrine Library," Joint Chiefs of Staff, accessed November 24, 2024, https://www.jcs.mil/Doctrine/.

5 See, for example: Heather S. Gregg, "The Human Domain and Influence Operations in the 21st Century," *Special Operations Journal* 2, no. 2. (2016):92-105.

What are the best practices in national-level efforts to help populations understand, prepare for, and cope with hybrid attacks against CI that hinder the delivery of critical goods and services?

This project aims to draw from Europe's experience building what it calls "societal resilience," which is the ability of populations to "resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of essential basic structures and functions."[6]

In addition to considering efforts by the North Atlantic Treaty Organization (NATO) and the European Union (EU) to prepare populations for the effects of hybrid threats, this research specifically investigates how Sweden, the United Kingdom (UK), and Romania have used a variety of tools to help protect their CI and prepare populations for disruptions in CI goods and services caused by hybrid attacks.

This project asks the following detailed questions:

- How do these countries define CI? What is included, what is not, and why?
- What are the range of hybrid attacks that these countries have had on their CI? How have these attacks disrupted goods and services?
- How do these countries educate their populations about hybrid war and potential attacks on CI, if at all?
- Who is responsible for this education (national government agency, non-governmental agency, etc.)? What role does the media play in educating the population?
- How is information delivered (SMS, radio, TV, printed, other)?
- What role, if any, does the private or non-governmental sector play in helping populations understand, prepare for, and cope with hybrid attacks that target CI?
- How does the level of trust between the population and the government affect messaging efforts?

To investigate these questions, the report is divided into four sections:

Section one provides an overview of what hybrid threats are, what CI is, and why adversarial hybrid attacks on CI are particularly challenging to governments.

Section two draws from academic and practitioner literature to consider how governments can help physically and psychologically prepare their populations for hybrid threats by building societal resilience to respond to these attacks in a way that quickly returns society to a healthy, functioning state.

Section three considers Europe's efforts to build societal resilience to withstand the disruption of goods and services caused by hybrid attacks against CI. It provides a brief overview of NATO requirements and EU directives for building resilience. It then investigates three countries' efforts to build resilience: Sweden, the United Kingdom, and Romania. These countries offer a range of approaches for building societal resilience and preparing populations for disruptions to goods and services caused by hybrid attacks against CI.

Section four provides a summary of the research and best practices for building societal resilience to withstand hybrid attacks against CI. Specifically, it identifies the following seven key takeaways:

1. **Define CI by its relationship to the population**

6 "Resilience," United Nations Office for Disaster Relief Reduction (UNDRR), accessed November 23, 2024, https://www.undrr.org/terminology/resilience#:~:text=The%20ability%20of%20a%20system,and%20functions%20through%20risk%20management.

There is no agreed-to definition of CI or which sectors should be designated as essential. Most definitions of CI include the four "lifeline" sectors of energy, water, communications, and transportation. A fifth lifeline of CI—financial infrastructure—should also be included when preparing populations for hybrid attacks on CI. Disruptions to the financial sector are a particular vulnerability that could be exploited by adversaries and cause mass panic in populations, especially if hybrid attacks prevent people from having access to their money, including being able to pay for items digitally and to withdraw cash.

Rather than specifically name sectors, Sweden defines CI by the critical services it provides and how disruptions of these services would affect populations. It calls this dynamic between CI and the population "vital societal functions." This functional definition helps governments understand the critical goods and services CI provides a population and prepare them for the effects of disruptions to these goods and services.

2. **Harden CI with good cyber strategies and defense against physical sabotage**

Cyberattacks are the most significant vulnerability to CI today, including distributed denial of service attacks (DDoS), ransomware, cyber espionage, and malware. Sweden, the UK, and Romania have developed cyber strategies, policies, and agencies for addressing cybersecurity, which should help with identifying, mitigating, and recovering from cyberattacks against CI. Public-private partnerships are also important to help mitigate the gaps and seams in CI and other related cybersecurity concerns.

Physical sabotage should not be overlooked as a potential hybrid attack against CI. Defending against physical sabotage requires strengthening the physical security of CI and improving intelligence aimed at identifying saboteurs and types of attacks on CI.

3. **Create policies and guidelines that establish a baseline of preparedness**

Crises, including hybrid threats, rarely stop at a country's borders. A crisis in one country will most likely affect neighboring countries, regions, and possibly the world. Russia's hybrid war against Ukraine and its allies, the European mass migration crisis of 2015, the Covid-19 pandemic of 2019–2022, and the 2025 power outage on the Iberian Peninsula are all examples of crises that crossed borders.

The EU and NATO have policies and guidelines designed to create a baseline of preparedness among member states against a range of threats, including hybrid threats to CI. Overarching efforts to create similar levels of preparedness across countries, regions, and alliances should, in theory, help mitigate disruptions of goods and services for a range of threats, both manmade and natural, and reduce possible "spillover" effects from one country or region to the next.

4. **Publicly call out states using hybrid threats against CI**

In Europe, Russia has capitalized on proxies and other third-party actors to mask their involvement in perpetrating a range of hybrid attacks against CI. Additionally, Russia has exploited gaps and loopholes in international law to carry out attacks, what is often called "lawfare."

Sweden, Romania, and the UK have all deliberately called out Russia as the state actor responsible for hybrid attacks against CI in their countries, despite the fact that most of these attacks cannot be legally proven to have come from the Kremlin.

Publicly calling out states believed to be behind cyberattacks and sabotage to CI is important for building consensus on the need for a political, economic, and military response to these attacks and "unmasking" states behind these acts. It is also an important step in explaining hybrid threats, preparing populations for these attacks, and demonstrating that governments are aware of the threat and fighting it.

5. **Physically and psychologically prepare populations for hybrid threats against CI**

   Building societal resilience requires physically preparing populations for disruptions of goods and services. This includes informing populations of the necessary goods to have for a specified amount of time, where to go in the event of specific crises, a communications strategy in the event of cellphone disruptions, and what to do in response to specific crises, including both natural and manmade disasters.

   As importantly, populations should be psychologically prepared. They should be educated about the nature of hybrid threats and the critical role they play in undermining these attacks by not "taking the bait" and panicking, turning on each other, or losing trust in the government. Put together, physically and psychologically preparing populations for the possibility of disruptions caused by hybrid attacks should reinforce one another and work to build societal resilience.

   Sweden and Romania have created guidebooks designed to prepare their populations for a spectrum of crises, ranging from dis- and mal-information to natural disasters to war and occupation. These guidebooks are short, issued in several languages, and include illustrations and simple-to-follow instructions, making them useful to the widest number of people. Sweden has mailed copies to each household to have on hand in the event of power and/or cellphone service disruption.

6. **Inform populations of their role in mitigating the effects of attacks against CI**

   Informing populations that they have a role to play in mitigating the effects of hybrid attacks is important, including acts against CI. If done properly, this should be empowering to the population and not frightening. Sweden, for example, emphasizes that, "To resist these threats, we must stand united…If Sweden is attacked, everyone must do their part to defend Sweden's independence—and our democracy. We build resilience every day, together with our loved ones, colleagues, friends, and neighbours."[7]

7. **Non-governmental organizations may be useful for consistent messaging**

   The UK and Romania have created independent, apolitical organizations dedicated to disaster preparedness and building societal resilience. These organizations may be helpful in providing continuity of information and messaging across administrations and in politically, ethnically, and socially divided countries.

Additionally, the report identifies the following three challenges:

1. **Finding the right balance for explaining hybrid threats is difficult**

   Governments and organizations need to find the right balance between threat, urgency, and empowerment when messaging the population about hybrid threats. If the threat is presented as too prevalent and

7 "In Case of Crisis or War," The Swedish Civil Contingencies Agency (MSB), 2024, https://rib.msb.se/filer/pdf/30874.pdf.

too dire, the message itself could cause populations to panic or react in a way that is negative to the normal functioning of society, what is known as "reflexive control." However, underselling the threat could cause people to not take the message seriously and not prepare.

Similarly, "crying wolf"—falsely predicting that a threat is imminent—might cause people to not take future messaging seriously, which could also result in populations not being prepared for crises.

Finding the right balance in messaging, therefore, is crucial and will most likely require country-specific, region-specific, and even population-specific messaging.

2. **Effectively messaging to populations requires a trusted messenger**

Sweden, the UK, and Romania have either politically or ethnically divided populations, or both. These divisions present challenges for finding trusted messengers that the whole population will listen to and follow instructions from.

To address political and ethnic divisions, Romania and the UK have both created apolitical organizations aimed at bridging ethnic and political divisions and sustaining messaging through changes in administrations, the Euro-Atlantic Resiliency Centre and the National Preparedness Commission, respectively.

Overall, preparing populations for disruptions of goods and services caused by hybrid threats requires a trusted messenger. If the government is not trusted by a portion of the population, additional messengers may be required.

3. **Creating measures of effectiveness (MOEs) for preparedness is challenging**

MOEs for preparing populations to withstand and recover from disruptions to goods and services caused by hybrid threats should include both physical preparedness and psychological preparedness.

Arguably, **physical preparedness** is easier to measure because it can include specified amounts per household of provisions, like food, water, medicine, fuel, and so on. Governments can instruct households how much to have on hand and then measure the effects of this messaging through surveys or other means.

MOEs for **psychological preparedness** are more difficult. In 2022, Sweden created the Psychological Defence Agency as a separate government entity to investigate and defend against "external information influence that is directed at Sweden with the aim of harming Swedish interests" and "to safeguard freedom of expression and open and democratic society."[8] Measuring effectiveness is part of their mission.

Historically, Sweden measures "the will to defend" as its principal means of psychological preparedness through household surveys, defining it as "a mental state during peacetime; measured at the individual level; how the individual relates to the group (society, community)" and as an "attitude of or capacity for standing against threats of violence." Sweden also includes conscription rates and attitudes toward territorial defense as metrics.[9]

8 "Our mission," Psychological Defence Agency (Government of Sweden), accessed July 7, 2025, https://mpf.se/psychological-defence-agency/about-us/our-mission.

9 Tarja Cronberg, "The Will to Defend: A Nordic Divide Over Security and Defence Policy," in *The Nordic Countries and the*

Creating the right MOEs for assessing populations' physical and psychological preparedness for disruptions of goods and services caused by hybrid threats remains a challenge that requires more study.

European Security and Defence Policy, eds. Alyson J. K. Bailes, Gunilla Herolf, and Bengt Sundelius (Oxford University Press, 2006), 315–322.

1. The Challenge of Hybrid Threats Against Critical Infrastructure

On May 7, 2021, specialists monitoring the Colonial Pipeline, a Houston, Texas-based facility that distributes gasoline across the southeastern United States, detected a security breach in its information technology (IT) system. The company quickly shut down its computer system and the distribution of gasoline through its 5,500 miles of pipelines. A hacking group calling itself "DarkSide" demanded 75 Bitcoin, approximately $4.4 million U.S. at the time, for the decryption key to the malware that had infected the system.

As news spread of the ransomware attack and Colonial Pipeline's decision to shut down the pipeline, panic began to set in across several states on the East Coast. Long lines formed at gas stations in Florida, Georgia, Alabama, Virginia, and the Carolinas, and people began to hoard gas. Online rumors circulated that some even tried to put gasoline in plastic shopping bags, prompting a national call for consumers to not engage in this activity. Gas stations began to run out of gas as consumers continued to panic buy, with some stations charging double the national average.[10] State authorities attempted to calm populations by assuring them that there was enough gas if people did not panic and hoard fuel. This message, however, did little to change behavior.[11]

On May 9, President Joseph Biden declared a state of emergency to address the crisis. Colonial Pipeline paid the ransom for the decryption key and resumed pumping gasoline throughout its system. President Biden addressed the nation on May 14 to assure the American people that the pipeline was running again and to explain federal measures designed to address fuel shortages. He implored, "Don't panic…I know seeing lines at the pumps or gas stations with no gas can be extremely stressful, but this is a temporary situation. Do not get more gas than you need in the next few days."[12] Eventually, consumer behavior returned to normal as it became clear that the crisis had ended. An FBI-led investigation suggested that DarkSide had connections to Russia, but these ties could not be definitively proven.[13]

Ultimately, the attack on the Colonial Pipeline may have been more than just a profit-seeking group's desire to extort money through ransomware. It may actually have been the act of a state working through "proxies"—individuals and groups that provide a degree of deniability to the state, and may or may not be working directly with the state—to execute illegal actions inside another state with the goal of causing panic and overreaction in the population, undermining the government's credibility, and weakening its ability to project power both internally and internationally.

Our European allies and partners call these activities "hybrid threats," which are hostile actions that are "coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities."

---

10 Christopher Brito, "Officials Warn People Not to Fill Plastic Bags with Gasoline Amid Panic Over Gas Shortage," CBS Evening News, May 14, 2021. https://www.cbsnews.com/news/gas-shortage-plastic-bags-warning-consumer-product-safety/.

11 Sean Michael Kerner, "Colonial Pipeline Hack Explained: Everything You Need to Know," *Techtarget*, April 26, 2022, https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.

12 "Remarks by President Biden on the Colonial Pipeline Incident," The White House, May 13, 2021.

https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/.

13 "FBI Deputy Director Paul Abbate's Remarks at Press Conference Regarding the Ransomware Attack on Colonial Pipeline," FBI National Press Office, June 7, 2021, https://www.fbi.gov/news/press-releases/fbi-deputy-director-paul-abbates-remarks-at-press-conference-regarding-the-ransomware-attack-on-colonial-pipeline.

Critically, these threats are "designed to remain below the threshold of detection and attribution," making a response difficult.[14]

Hybrid threats against CI, like the Colonial Pipeline, are especially challenging for governments because they are difficult to prevent and not only affect a population's access to critical goods and services but also diminish their trust in the government's ability to protect CI and provide these goods and services when attacks occur. Furthermore, when executed effectively, the population's response to hybrid threats becomes part of the attack itself. Populations panic, amplifying the attack, and force governments to devote time and resources to restore order, as was the case with the Colonial Pipeline incident.

A 2023 report published by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) underscores the vulnerabilities the U.S. faces with persistent threats to CI and the need to prepare the population for these attacks. Citing the 2023 U.S. National Intelligence Estimate (NIE), the CISA report asserts that, "If Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure."[15] Drawing from this NIE threat assessment, CISA argues that "we need to normalize cyber risks for the general public with the recognition that cyber-attacks are a reality for the foreseeable future. We cannot completely prevent attacks from happening, but we can minimize their impact by building resilience into our infrastructure *and into our society.*"[16]

This report investigates how hybrid threats against CI are a particular vulnerability to countries today and how governments can prepare their populations for disruptions to goods and services caused by these attacks.

To help explain this form of warfare, the report begins by providing a brief overview of key Terms, including what hybrid threats are, why populations are one of the principal targets of hybrid threats, and why CI is an especially attractive target for hybrid attacks.

Key Terms

First, the term **grey zone** is often used to describe the space where a range of nefarious activities are occurring. U.S. Special Operations Command, for example, defines the grey zone as "competitive interactions among and within state and non-state actors that fall between the traditional war and peace duality."[17] Somewhat similarly, the Center for Strategic International Studies defines the grey zone as "the contested arena somewhere between routine statecraft and open warfare."[18] David Kilcullen's concept of "liminal zones," which are similar to the grey zone, identifies several levels of activity and attribution, ranging from clandestine (action undetected) to covert (action detected but unattributable) to ambiguous (action detected, actor suspected but unprovable) to overt (both action and actor visible). The space between these different types of attacks presents challenges for formulating a response in a timely and proportional way while not inadvertently or accidentally escalating the

14 Hybrid COE, "Hybrid threats as a concept."
15 Jen Easterly, "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years," Cybersecurity & Infrastructure Security Agency, May 7, 2023, https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.
16 Easterly, "The Attack on the Colonial Pipeline." Emphasis added.
17 "The Gray Zone."
18 "Gray Zone Project," Center for Strategic & International Studies, accessed March 21, 2025, https://www.csis.org/programs/gray-zone-project.

conflict.[19] The grey zone, in other words, is the space between open war and unchallenged peace where a range of hostile activities occur.

Irregular warfare is the overarching concept that describes a range of hostile activities that occur in the grey zone and fall outside traditional state-on-state warfare between uniformed, organized militaries. U.S. Joint Doctrine 1 Vol. 1, "Joint Warfighting" (2023) defines irregular warfare as "a form of warfare where state and non-state actors campaign to assure or coerce states or other groups through indirect, non-attributable, or asymmetric activities, either as the primary approach or in concert with conventional warfare."[20] The concept of irregular warfare, critically, includes a range of hostile activities that are "indirect." The Irregular Warfare Center, for example, draws on U.S. doctrine and similar guidance to include activities such as terrorism, cyberattacks, sabotage, insurgency, guerilla warfare, and proxy warfare as examples of indirect activities in irregular warfare.[21]

Hybrid threats are a specific subset of activities within irregular warfare. Perhaps the most cited definition of hybrid threats comes from the Helsinki Hybrid Center of Excellence (Hybrid COE), which was created in 2017 as a collaborative effort between NATO, the EU, and partnering nations to address a range of hostile activities in the wake of Russia's illegal annexation of Crimea and eastern Ukraine. Hybrid COE defines hybrid threats as a "concept" that

> *…refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution.*[22]

Hybrid COE's concept stresses that hybrid threats aim to "deliberately target democratic states' and institutions' vulnerabilities" with the overall goal of undermining a country's political system, and that they are coordinated and synchronized to have this effect. Hybrid threats, in other words, could be just about anything, so long as they have the wider effect of undermining the social and political unity of the country and preventing states from projecting power inward and internationally.[23] Mark Galeotti famously calls this "the weaponization of everything."[24]

The Hybrid COE "concept" further stresses that hybrid threats are difficult to detect and attribute to an actor. Swedish scholar Mikael Weissmann echoes this observation, stressing that "deception and denial are inherent in hybrid methods, and it is sometimes difficult to know for sure that warfare is ongoing, and in the same way, it is inherently difficult to identify if, and when, a perceived threat of future action becomes reality."[25]

---

19 David Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West* (Oxford University Press, 2020).
20 "Joint Doctrine Library."
21 "Irregular Warfare 101 Course," Defense Security Cooperation University, accessed April 14, 2025, https://dscu.edu/course-catalog/course/13271.
22 Hybrid COE, "Hybrid Threats as a Concept." Other terms used to describe this range of hostile activities is political warfare, a term used by U.S. statesman George Kennan. See: "269. Policy Planning Staff Memorandum," May 4, 1948, https://history.state.gov/historicaldocuments/frus1945-50Intel/d269. China uses the term "unrestricted warfare". See: Mark Thomas, "The Chinese Roots of Hybrid Warfare," *CEPA*, August 10, 2022. https://cepa.org/article/the-chinese-roots-of-hybrid-warfare/, as of January 20, 2025.
23 Heather S. Gregg, "Hybrid Threats and Strategic Competition," *Connections QJ* 23, no. 2 (2024): 159–171.
24 Mark Galeotti, *The Weaponization of Everything: A Field Guide to the New Way of War* (Yale University Press, 2022).
25 Weissmann, "Conceptualizing and Countering Hybrid Threats and Hybrid Warfare," 63.

Several scholars argue that distinguishing **hybrid warfare** from hybrid threats is important for understanding the unique challenges of each form of warfare. The International Institute for Strategic Studies defines hybrid warfare as:

> *The use of military and nonmilitary tools in an integrated campaign designed to achieve surprise, seize the initiative and gain psychological as well as physical advantages utilizing diplomatic means; sophisticated and rapid information, electronic and cyber operations; covert and occasionally overt military and intelligence action; and economic pressure.*[26]

Hybrid warfare, therefore, involves more visible activities, such as positioning troops and the actual use of force, but also includes the range of undetectable and unattributable activities of hybrid threats within the adversary's overall strategy. Furthermore, in hybrid warfare, the population is directly targeted, in addition to fighting another country's military.

Somewhat confusingly, NATO's definition of hybrid threats uses hybrid threats and hybrid warfare interchangeably:

> *Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber attacks, economic pressure, deployment of irregular armed groups and use of regular forces. Hybrid methods are used to blur the lines between war and peace, and attempt to sow doubt in the minds of target populations. They aim to destabilise and undermine societies.*[27]

Nevertheless, this report will use these terms distinctly and will focus specifically on hybrid threats to CI in countries that are not experiencing open warfare. When a hybrid threat is executed, it becomes a **hybrid attack**. This report will argue that hybrid threats are part of a wider strategy of targeting populations to undermine the government's credibility and weaken its ability to project power internally and internationally.

As will be described further below, a population's response to a hybrid attack is a critical part of the adversary's plan. Adversaries target populations with the hope that they will panic, overreact, and blame their governments for a lack of preparedness and the inability to stop the attack. In essence, the population's response becomes part of the strategy. Therefore, preparing populations for hybrid attacks that disrupt goods and services helps to undermine the adversary's plan.

Critical Infrastructure

Hybrid attacks on CI are an especially powerful tool for state and nonstate actors wishing to challenge another state below the threshold of armed conflict because these attacks accomplish several goals at once: they damage CI that delivers goods and services to populations without clear attribution to the perpetrating state; they sow fear and uncertainty within the population, requiring governments to commit more resources and attention inward to address these concerns and challenges; and they make governments look unprepared and ineffective in protecting their CI and their populations, undermining the governments' legitimacy.

Protecting CI from hybrid threats has several challenges. First, there is little consensus among states on which specific sectors should be included as CI and why. One definition describes CI as "the physical and cyber

26 Weissmann, "Conceptualizing and Countering Hybrid Threats and Hybrid Warfare," 64.

27 "Countering Hybrid Threats," North Atlantic Treaty Organization, accessed December 6, 2024, https://www.nato.int/cps/en/natohq/topics_156338.htm.

systems and assets that are so vital to a country that their incapacity or destruction would have a debilitating impact on a nation's physical or economic security or public health and safety."[28] Given this definition, countries will have their own lists of what comprises CI based on geography, infrastructure, population, vulnerabilities, and needs. For example, in the United States, CISA identifies sixteen sectors in critical infrastructure: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government services, healthcare and public health, information technology, nuclear reactors (including material and waste), transportation systems, and water and wastewater.[29]

Despite the variation in country-specific designation of CI, there is a general consensus that four broad sectors constitute a "critical lifeline" for most countries: energy, water, transportation, and communications infrastructure.[30] These four broad sectors typically include several specific services within each. For example, transportation includes roadways, bridges, buses, railways, airports, waterways, and seaports, depending on geography. Therefore, even within these four critical sectors, there will be variation in specific services depending on the size and geography of the country.

As will be discussed further below, a fifth sector of CI—financial infrastructure—should also be included when preparing populations for and recovering from hybrid attacks on CI. Disruptions to the financial sector—DDoS attacks, ransomware, GPS jamming, and other hybrid attacks—are a particular vulnerability that could be exploited by adversaries and cause mass panic in populations, especially if these attacks prevent people from having access to their money, including being able to pay for items digitally and to withdraw cash.[31]

Second, most countries' CI includes a mixture of government and privately owned companies and enterprises, making protecting CI challenging. These partnerships require delineation of who is responsible for protecting services, including both formal laws and authorities as well as collaboration through less formal channels before attacks occur, and plans and procedures for what to do once attacks on privately provided CI do occur.

Third, CI is almost always interconnected; an attack on one sector most likely will affect other sectors as well, causing a cascading crisis. For example, electricity is required to run virtually every other CI sector in any given country and, while generators and other temporary sources of power can provide electricity in times of crisis, major disruptions to a country's supply of electricity will have cascading effects across CI sectors.[32]

Fourth, failures of CI in one country can also affect CI in other countries. For example, in 2017, the Danish shipping company Maersk was hit with a cyberattack that took down their computer system, paralyzing their operations for days, shutting down ports, and affecting shipping around the world. The malware, called "NotPetya," was attributed to a hacking group with ties to the Russian military that intended to hit Ukrainian CI but infected and disrupted the Danish shipping company's computer system as well.[33]

---

28 Ronald Bearse, "Understanding Critical Infrastructure," in *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency,* ed. Carol V. Evans (U.S. Army War College Press, 2022), 1–2.

29 "Critical Infrastructure Sectors," Cybersecurity and Infrastructure Security Agency, accessed March 22, 2025, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

30 Carol Evans, "Executive Summary," in *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency*, ed. Carol V. Evans (U.S. Army War College Press, 2022), xxiii.

31 See, for example: Jeff Coffed, "The Theat of GPS Jamming: The Risk to an Information Utility," *Exelis*, February 2024, https://rntfnd.org/wp-content/uploads/Exelis-GPS-Vulnerability-Assessment-February2014.pdf.

32 For a scenario involving prolonged lack of electricity and its cascading effects, see: Cedric De Coning, "Hybrid COE Working Paper 9: Strengthening the Resilience and Adaptive Capacity of Societies at Risk from Hybrid Threats," Hybrid COE, June 2021, https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-9-strengthening-the-resilience-and-adaptive-capacity-of-societies-at-risk-from-hybrid-threats.

33 Mike McQuade, "The Untold Story of NotPetya: The Most Devastating Cyber Attack in History," *Wired*, August 22, 2018,

Fifth, predicting hybrid attacks against CI is difficult if not impossible to do. Most countries prioritize protecting CI from a range of threats, including both natural and manmade disasters, to ensure that essential goods and services are delivered to their populations. Some of these threats are more predictable than others. Hurricanes, for example, are a fairly predictable threat. Statistics maintained by the National Oceanic and Atmospheric Agency (NOAA) show that hurricane season in the U.S. runs roughly from the beginning of June to the end of November, with the peak season from mid-August to mid-September. Florida experiences the most hurricanes, followed by Texas and the Carolinas.[34] Each year, NOAA makes predictions on the number of hurricanes and tropical storms based on statistics and atmospheric conditions. While not all hurricanes and tropical storms conform to these specifics, states and federal agencies can prepare for this natural disaster and mitigate its effects, including on CI.

Other natural disasters are less predictable. Earthquakes, for example, cannot be forecasted.[35] However, regions that are prone to these activities can take preparatory and defensive measures to secure CI. For example, in California, all new buildings must conform to safety standards that make them more resilient to seismic activity.[36]

Overall, natural disasters tend to be regionally specific. Hurricanes typically affect coastal regions. Earthquake-prone regions are also identifiable, as are areas with volcanic activity. This allows countries and regions to prepare for these events, including making CI more resilient to natural disasters and thus minimizing disruptions to goods and services.

Hybrid attacks against CI, however, can occur anywhere at any time, making prevention very difficult, if not impossible. Cedric de Coning of the Norwegian Institute of International Affairs summarizes this difference between natural disasters and hybrid threats:

> *One can prepare for natural disasters like fire, floods, earthquakes, and so on because although it may not be known when they might occur, they are natural events that follow certain known patterns. Hybrid threats differ in that they are human-induced and designed to cause maximum social disruption…*[37]

Put another way, unlike with natural disasters, the perpetrators of hybrid attacks are humans with specific intentions.

Given the intentionality of hybrid attacks and the key role that the population's response plays, it may be more useful to compare hybrid attacks against CI to terrorism than to natural disasters. NATO's definition of terrorism illustrates this point well. It defines terrorism as: "The unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives."[38] Terrorist acts bear similarity to hybrid attacks on CI because they both aim to instill fear in populations and

---

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

34 "Tropical Cyclone Climatology," National Oceanic and Atmospheric Agency, accessed March 25, 2025, https://www.nhc.noaa.gov/climo/#:~:text=The%20official%20hurricane%20season%20for,%2DAugust%20and%20mid%2DOctober.

35 "19-01: Seismic Safety Commission Building Code and Earthquakes," California SSC, accessed March 25, 2025, https://ssc.ca.gov/wp-content/uploads/sites/9/2020/08/ssc19-01.pdf.

36 "Can You Predict Earthquakes?" U.S. Geological Society, accessed March 25, 2025, https://www.usgs.gov/faqs/can-you-predict-earthquakes#:~:text=Unfortunately%2C%20most%20such%20precursors%20frequently,be%20made%20in%20probabilistic%20terms.

37 De Coning, "Strengthening the Resilience and Adaptive Capacity of Societies at Risk from Hybrid Threats," 15.

38 For NATO's definition of terrorism, see: "NATO's Military Concept for Defence Against Terrorism," North Atlantic Treaty Organization, August 19, 2016, accessed March 22, 2025, https://www.nato.int/cps/en/natohq/topics_69482.htm#:~:text=The%20unlawful%20use%20or%20threatened,political%2C%20religious%20or%20ideological%20objectives.

cause them to panic. However, groups perpetrating terrorist attacks typically claim responsibility for the attack as a form of publicity and recruitment. In hybrid attacks, states will aim to conceal their involvement to prevent legal actions or counterattacks.

Both manmade and natural disasters require governments and the private sector to protect CI with the aim of preventing damage and ensuring critical goods and services are delivered to populations. With the growing complexity of CI, especially its dependence on computers to function, defending CI is typically described as ensuring both its security and resilience, what is known as CISR. CI expert Ronald Bearse says,

> *Security means reducing the likelihood of physical attacks against of critical infrastructure or the effects of natural or man-made disasters through the application of physical means or cybersecurity measures. Resilience is the ability of critical infrastructure to resist, absorb, recover from, or successfully adapt to changing conditions.*[39]

CISR, therefore, involves a mixture of risk assessment, protection, and plans to restore CI quickly in the event it is damaged from natural or manmade disasters, including hybrid attacks.

Despite the best plans to provide security and resilience to CI, accidents, natural disasters, human errors, and intentional attacks cannot be completely prevented. Populations, therefore, need to be prepared for disruptions to critical goods and services provided by CI, irrespective of the cause of disruption.

Preparing populations to defend against, withstand, and recover from hybrid attacks against CI is especially important because the adversary most likely is expecting the population to panic, thus amplifying the attack. As Cedric de Coning put it, hybrid threats are "…human-induced and designed to cause maximum social disruption."[40]

The 2021 Colonial Pipeline attack illustrates this point well. If the population had been psychologically prepared for such an attack, had understood its likely purpose, and had confidence that the pipeline's services would be restored, the effects of the attack would have been less severe.

Key Takeaways:

- **Hybrid threats** are coordinated and synchronized actions short of open warfare that deliberately target a country's vulnerabilities. State actors, often working through proxies, use a wide range of means designed to remain below the threshold of detection and attribution to undermine countries and affect their ability to project power. Populations are the principal target of hybrid threats.
- **Defining CI** varies by country and depends on geography and other variables. Most definitions of CI include the four "critical lifeline" sectors of energy, water, transportation, and communications infrastructure, along with their subcomponents. A fifth sector of CI—financial infrastructure—should also be included when preparing populations for hybrid attacks, especially if these attacks prevent people from having access to their money, including being able to pay for items digitally and to withdraw cash, which is likely to cause mass panic.
- **Hybrid threats against CI** are a powerful means of targeting populations inside a country because attacks can be conducted anonymously either through cyberattacks or physical sabotage, and attacks on CI can cause major disruptions to goods and services.

39 Bearse, "Understanding Critical Infrastructure," 7–8.
40 De Coning, "Strengthening the Resilience and Adaptive Capacity of Societies at Risk from Hybrid Threats," 15.

- **Hybrid attacks against CI can occur anywhere and at any time**, making prevention very difficult, if not impossible. Preventing attacks is also challenged by public-private ownership and management of CI, including gaps in responsibilities and authorities. Additionally, attacks in one sector can have cascading effects in other sectors, and attacks on CI in one country can cross borders, requiring coordination in prevention, crisis management, and recovery.
- Given the intentionality of hybrid attacks and the key role that the population's response plays, it may be more useful to **compare hybrid attacks against CI to terrorism than to natural disasters**.

The next section will consider how to build societal resilience to prepare populations for disruptions to critical goods and services caused by hybrid attacks to CI.

2. Preparing Populations for Hybrid Attacks Against CI

As described in the previous section, the growing frequency of hybrid attacks against a country's CI makes completely preventing these attacks virtually impossible. Hybrid threats are a powerful way for adversaries to cause panic and fear within a population and undermine their trust in their government, especially if the government is unable to quickly restore goods and services to the population. Preparing the population to withstand and recover from hybrid attacks that disrupt goods and services is thus an important means of interdicting the adversary's plans.

This section explores the concept of **societal resilience**, why it is so important for blunting the strategy of adversaries who use hybrid threats against CI, and how states can help populations understand, prepare for, and recover from the effects of these attacks. It looks at four broad programs aimed at building societal resilience in the United States: civil preparedness during the Cold War; preparing populations for terrorist incidents after the 9/11 attacks in New York and Washington, DC; natural disaster preparedness; and measures taken to inform and prepare people to withstand the Covid-19 pandemic.

These programs offer clues for how the United States could prepare its population for hybrid attacks against CI that cause disruptions to goods and services and what some of the challenges may be. Specifically, it underscores the importance of preparing populations *before* a crisis occurs, both physically and psychologically, for disruptions to goods and services. Preparing the population and building societal resilience ahead of these crises is key to preventing counterproductive behavior and returning society to normal as quickly as possible. Furthermore, research on the Covid-19 pandemic suggests that the degree of trust between the population and the government is positively correlated with its willingness to follow the government's instructions. In other words, the more the population trusts the government, the more likely it will follow its instructions and, conversely, the less the population trusts the government, the less likely it will follow instructions.

What Is Societal Resilience?

The previous section described the importance of states moving beyond mere physical protection of CI to the broader concept of CISR, which also includes security and risk assessment for preventing physical and cyberattacks on CI, and building infrastructure resilience, which is its ability to "resist, absorb, recover from, or successfully adapt to changing conditions."[41]

CISR, however, does not directly include the vital role that the population plays in responding to hybrid attacks and returning both CI and society to a normal, functioning state after a crisis. Because not all attacks against CI can be prevented, it is critically important to prepare populations for the disruption of goods and services these attacks may cause. Preparing the population for the effects of these attacks should help minimize the crisis and undermine the adversary's strategy.

The capability and capacity of a population to withstand and recover from various threats, including both natural and manmade disasters, is called **societal resilience**. The United Nations Office for Disaster Risk Reduction (UNDRR) defines societal resilience as "the ability of a community or society exposed to hazards

41 Bearse, "Understanding Critical Infrastructure," 7–8.

to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of essential basic structures and functions."[42]

De Coning provides a specific definition of societal resilience in the context of hybrid threats, what he calls "**civilian resilience**," which is "the ability of a society to prevent, manage and recover from hybrid attacks without losing its essential values, cohesion and identity."[43] De Coning pairs civilian resilience with adaptive capacity, which is "the ability to thrive in an environment characterized by change," and social capital, or "networks together with shared norms, values and understandings that facilitate co-operation within or among groups," as the necessary foundation upon which societies can respond to and recover from hybrid threats.[44] De Coning's definition is particularly valuable because it identifies what is the target of hybrid threats—"essential values, cohesion, and identity" of a population—and therefore what must be defended and restored in the event of a successful hybrid attack. These key targets of hybrid threats will be included in discussions of societal resilience, which is the more commonly used term.

Notably, building societal resilience includes more than just withstanding disruptions of goods and services caused by hybrid attacks on CI. This preparation should also cover any event that causes disruptions to goods and services, such as natural disasters, pandemics, accidents, and human errors, as well as hybrid threats—what is sometimes called an "all hazards approach."[45] Additionally, building societal resilience extends beyond just preparing for a disruption in goods and services caused by damage to CI. It also includes educating the population to identify and withstand mal- and disinformation,[46] and even prepare for conventional and nuclear war. In some countries, preparing populations for a range of threats to the homeland is called **total defense**, **comprehensive defense**, **civil defense**, or **civil preparedness**.[47] However, the concept of societal resilience is arguably the broadest term for preparing populations for a range of threats; for this reason, this is the term that this report will use.

Building societal resilience is not a new concept. Several European countries have programs that extend back to World War I that, while not called societal resilience, were designed to build fortitude in populations to withstand aerial bombardments and other forms of combat that involved populations.[48] Furthermore, most European countries, including former Soviet and Soviet satellite countries, had civil defense programs throughout the Cold War, which were designed to prepare populations for conventional and nuclear war. The 1949 NATO Treaty included the concept of societal resilience as part of Article 3, which calls for member states to maintain resilience and civil preparedness within their own countries as part of collective defense, and as a

42 "Resilience," UNDRR.

43 De Coning, "Strengthening the Resilience and Adaptive Capacity of Societies at Risk from Hybrid Threats," 17.

44 De Coning, "Strengthening the Resilience and Adaptive Capacity of Societies at Risk from Hybrid Threats," 17–18.

45 Mikael Wigell, Mariette Hägglund, Christian Fjäder, Emma Hakala, Johanna Ketola, and Harri Mikkola, "Nordic Resilience: Strengthening Cooperation on Security of Supply and Crisis Preparedness," *FIIA Report*, No. 70, September 2022, https://fiia.fi/en/publication/nordic-resilience.

46 Disinformation is incorrect information deliberately spread to cause harm. Mal-information is true information deliberately spread to cause harm, and misinformation is false information spread without the intention to cause harm. Information as HT involves intention and, therefore, disinformation and mal-information are the better terms. See: Claire Wardle, "Understanding Information Disorder," *First Draft News*, September 22, 2020. https://firstdraftnews.org/long-form-article/understanding-information-disorder/.

47 Sweden, for example, has the concept of "Total Defence," which includes civil defense and military defense. See: "Total Defence," Government Offices of Sweden, accessed March 26, 2025, https://www.government.se/government-policy/total-defence/.

48 See, for example: "Civil Defense: From the Cold War to Contemporary Threats," Virginia Department of Emergency Management, accessed March 26, 2025, https://www.vaemergency.gov/aem/blue-book/civil-defense-from-the-cold-war-to-contemporary-threats.pdf.

means of supporting deterrence against outside aggression.[49] And the United States had a civil defense program that aimed to prepare populations for what to do in the event of a nuclear war.

Therefore, while building societal resilience is not necessarily a new concept, it is a new term that has taken on increased importance in the age of hybrid threats as a way of minimizing panic in populations and undermining the adversary's wider strategy of weakening a state and preventing it from projecting power.

U.S. Programs for Preparing Populations for Disasters

Programs that aim to inform and prepare populations for hybrid threats against CI are a critical means of creating societal resilience. Critically, the goal of these programs should be to prepare populations *before* a crisis occurs, so that they know what to do when an attack happens. These programs, in other words, are different from crisis management or crisis communications, which aim to message and coordinate a response once a crisis has occurred. Preparing a population before a crisis, in theory, should minimize the crisis and speed up recovery time, thus undermining the adversary's attempts to cause societal disruption.

Four U.S. programs aimed at preparing citizens for a range of disasters and building societal resilience are useful for this investigation: civil defense education during the Cold War; efforts to inform U.S. citizens about terrorist attacks after 9/11; preparation for natural disasters; and the response to the Covid-19 pandemic. Each of these programs offers insights into and challenges for how to prepare U.S. citizens for disruptions to goods and services caused by hybrid attacks against CI and build societal resilience.

1. Civil defense education during the Cold War. In the United States, the "Federal Civil Defense Act of 1950 and 1951" introduced a range of measured designed to prepare the public for the possibility of nuclear war. The Act called for the creation of civil defense communications and an early warning system along with stating that the government should "publicly disseminate appropriate civil defense information by all appropriate means."[50]

The Act provided federal funds for movies, radio broadcasts, and printed educational materials designed to inform and instruct populations in the event of a nuclear attack. The 1951 short movie "Our Cities Must Fight," for example, aimed to prepare populations in cities for war by encouraging neighborhoods to create volunteer civil defense corps instead of panicking and "taking to the hills," which would block roads and prevent first responders from reaching affected areas. The movie stressed that defeating the enemy's plans required citizens to stay in cities. The population's response, in other words, was seen as important for mitigating the effects of the attack.[51] The 1951 animated movie "Duck and Cover" provided guidance to young audiences for what to do in a nuclear attack. The movie introduced "Bert the Turtle," who sang a song that included the phrase "duck and cover" to help children prepare for nuclear war.[52] The 1950 booklet "Survival Under Atomic Attack" was also

49 Although it does not specifically use this term. Article 3 of the NATO Charter states: "In order more effectively to achieve the objectives of this Treaty, 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." See: "Resilience, Civil Preparedness and Article 3," North Atlantic Treaty Organization, November 13, 2024, accessed March 23, 2025, https://www.nato.int/cps/bu/natohq/topics_132722.htm.

50 "Federal Civil Defense Act of 1951," 81st Congress (1951), 1248–1249.

51 *Our Cities Must Fight,* written by Ray J. Mauer, directed by Anthony Rizo (Archer Productions, 1951), https://archive.org/details/OurCitie1951.

52 *Duck and* Cover, written by Raymond J. Mauer, directed by Anthony Rizo (Archer Productions, 1951), accessed April 8, 2025, https://www.youtube.com/watch?v=IKqXu-5jw60.

created during this time to explain how to prepare for and survive a nuclear attack, including where to go and what to have on hand.[53]

Academic literature that analyzes U.S. civil preparedness during the Cold War debates the efficacy and controversy of such programs. Kenneth Rose, for example, chronicles U.S. efforts to fund and develop fallout shelters, including messaging aimed at encouraging families to build their own shelters to defend against nuclear war. Overall, he argues that these efforts to prepare for nuclear war were unsuccessful in procuring federal and state funding and did little to successfully encourage families to take action.[54]

Psychiatrist Mary E. Woesner provides evidence that civil defense messaging, especially "Duck and Cover," actually traumatized a generation of children and did little to prepare them for nuclear war. She cites data from the 1980s to assert that "the emotions of those who had experienced the drills ranged from bewilderment to fear to 'helplessness and a sense of powerlessness, as well as a profound sense of fear about the future.'" [55]

Finally, measuring the effectiveness of Cold War messaging to prepare populations for the possibility of nuclear war is challenged by the fortunate reality that the United States never experienced nuclear war and therefore precisely measuring preparedness against an actual nuclear crisis did not occur.

2. Mass terrorism. The rise of mass terrorism following the 9/11 attacks in the United States prompted new efforts to prepare populations for terrorism-related disasters.

As of 2025, the U.S. Federal Emergency Management Agency (FEMA) is the government agency responsible for coordinating preparations and response to terrorist incidents, along with other manmade and natural disasters. Prior to 9/11, FEMA helped with the response to several mass causality terrorist incidents, most notably the April 1995 bombing of the Alfred P. Murrah federal building in Oklahoma, which killed 168 people. A 2001 Government Accountability Office (GAO) report, which was issued a few months before the 9/11 attacks, noted that FEMA had made considerable progress in preparing for a mass terrorist attack.[56] Despite this, 9/11 still caught federal and state authorities, as well as the general public, off guard.

Following 9/11, the Ad Council, a nonprofit organization founded in during World War II with the mission "to convene the best storytellers to educate, unite and uplift…by opening hearts, inspiring action and accelerating change," released a series of public service announcements (PSAs) designed to shape behavior of Americans in the wake of the attacks.[57]

One advertisement, "The Future is in Our Hands," begins by stating, "They have brought the battle here. They have attacked us in our homes and in our hearts…and it is here that we will defeat them." The ad shows Americans at work, in schools, walking down busy streets, and resuming normal life, suggesting that this is one

53 "Survival Under Attack," U.S. National Security Research Board Civil Defense Office, 1950, https://orau.org/health-physics-museum/files/library/civil-defense/survival-under-atomic-attack.pdf.

54 Kenneth D. Rose, *One Nation Underground: The Fallout Shelter in American Culture* (NYU Press, 2001).

55 Mary E. Woesner, "The Return of Duck and Cover, and the Imminence of Death—What It Means for Physicians," *JAMA Pediatrics* 172, No. 6 (June 2018): 511–512.

56 "Combating Terrorism: FEMA Continues to Make Progress in Coordinating Preparedness and Response," Government Accountability Office, March 20, 2001. https://www.gao.gov/products/gao-01-15.

57 "Our History," The Ad Council, accessed June 20, 2025, https://www.adcouncil.org/.

of the most important ways to demonstrate that the enemy has not succeeded in sowing fear and panic in the population.[58]

Another advertisement shows a neighborhood street with a voiceover that states "On September 11th, the terrorists tried to change America forever…" The street then shows American flags hanging from every house with the words, "well…they succeeded," suggesting that the attacks backfired, and Americans were more united and resilient than ever.[59]

Yet another advertisement, "I am an American," shows people of all races and ethnicities stating "I am an American" in an effort to underscore the strength of U.S. diversity and undermine narratives that could lead to disunity.[60] The impact of the "I am an American" campaign was unavailable on the Ad Council website.[61] However, one scholar noted controversy surrounding the campaign, specifically the concept of "diversity patriotism" and that it inadvertently identified some Americans as "safe" and others as "unsafe."[62]

In New York City, the Metropolitan Transportation Authority introduced "If you see something, say something" after the 9/11 attacks, which was designed to prepare populations to be vigilant on subways and other forms of mass transit, including identifying and reporting suspicious behavior, and what to do if you see an unattended bag. This campaign was later adopted by the U.S. Department of Homeland Security and became a nation-wide program. The information campaign included several ways to leave tips and easy reporting instructions.[63] Terrorism experts Brian Michael Jenkins and Bruce R. Butterworth argue that this campaign has been successful in stopping terrorist attacks. "By discovering and reporting suspicious objects, [individuals] have prevented more than 10 percent of all terrorist attacks on public surface transportation," they wrote. "Detection rates are even better in the economically advanced countries where more than 14 percent of the attempts are detected."[64]

In 2003, the RAND Corporation published *Individual Preparedness and Response to Chemical, Radiological, Nuclear, and Biological Terrorist Attacks*, which provides a "what if" scenario for each type of attack, a brief explanation of the unique threats these agents pose, and quick actions to take in the event of an attack. It is unclear, however, if this manual was distributed beyond RAND's website.[65]

The American Red Cross also issued guidance for preparing for terrorist attacks after 9/11, called "Terrorism Preparedness." Its website includes what might happen in a terrorist attack, including mass casualties, the need for enhanced law enforcement, school closures, and so on. It includes preparations for a terrorist incident, including a list of items to keep on hand; the need for a meeting and a communication plan; what to do in the event of a terrorist attack, including what to do in the event of mandatory evacuations; and what to expect after

58 "The Future is in Our Hands," The Ad Council, accessed April 8, 2025, https://www.youtube.com/watch?v=OdmCF20RfeU.

59 "Freedom Ads After the 9/11 Attacks," The Ad Council, accessed April 8, 2025, https://youtu.be/YkKWjyHoqyA?si=Vvc7e6_v5Wi7beXD.

60 "I Am an American," The Ad Council, accessed April 14, 2025, https://www.youtube.com/watch?v=F-81ObJYj70.

61 The Ad Council measures the impact of its ads "through a dashboard of indicators around exposure, awareness, engagement, and impact, employing test-and-learn practices throughout." See: "Measuring Impact," The Ad Council, accessed June 20, 2025, https://www.adcouncil.org/our-impact/measuring-impact.

62 Cynthia Weber, "I am an American: Protesting Advertised 'Americanness,'" *Citizenship Studies*17, no. 2 (2013): 278–292.

63 "If you see something, say something," U.S. Department of Homeland Security, accessed April 8, 2025, https://www.dhs.gov/see-something-say-something.

64 Brian Michael Jenkins and Bruce R. Butterworth, "Does "See Something, Say Something" Work?" Mineta Transportation Institute, SP11-18, December 2018. https://transweb.sjsu.edu/research/SP1118-See-Something-Say-Something.

65 Lynne Davis, et al, *Individual Preparedness and Response to Chemical, Radiological, Nuclear, and Biological Terrorist Attacks* (RAND, 2003). Of note, I was working for RAND on counterterrorism at the same time this manual was created and did not hear about it.

an attack, including heavy law enforcement and possible prolonged disruptions to daily activities. The website also includes downloadable PDFs with detailed information, and an emergency app for smart phones.[66]

As of 2025, the United States has not experienced another major terrorist attack on the scale of 9/11. Precisely measuring the effects of programs designed to prepare the population for major attacks, therefore, is difficult.

3. Natural disaster preparedness. Finally, there is a sizable body of literature that offers guidance and best practices in preparing populations for natural disasters, especially the role of educating and preparing the population before a disaster occurs.

As of 2025, FEMA is the national-level organization responsible for preparing the United States for disasters, both natural and manmade, aiding the response during a disaster, and helping recovery.[67] FEMA's website summarizes, "we work with individuals and communities to build a culture of national preparedness through active community engagement, trainings and education, and planning." This includes providing downloadable brochures for "12 Ways to Prepare," a FEMA app for smartphones, and training and education programs.[68]

FEMA's slow response to Hurricane Katrina's disastrous effects in New Orleans and the surrounding areas in 2005 prompted several investigations into its practices, including how it informs the public. The GAO, for example, conducted investigations of FEMA in 2006, 2015, and 2019 to monitor how it prepared populations for disasters and helped facilitate recovery after a disaster occurred. Overall, these reports show FEMA has made progress since 2005; however, it continues to experience challenges with staffing and with providing adequate outreach to communities to prepare them for a range of disasters.[69]

To better measure its effectiveness, FEMA began conducting the annual National Household Survey in 2013, which is designed to measure disaster preparedness through questions that gauge the public's knowledge of what do to in the event of a disaster, the amount of goods they have intentionally set aside for disasters, and if they have signed up for emergency broadcasts, among other questions.[70] The 2024 survey finds that fifty-seven percent of respondents reported that "I am NOT prepared [for a disaster], and I do not intend to prepare in the next year."[71] However, the same survey also revealed that "69 percent of respondents had assembled supplies to use in the event of an emergency," and "88 percent of respondents who had assembled supplies reported that their supplies could last for more than three days."[72] Regarding manmade disasters, sixty-three percent named a power outage as their principal concern, with thirty-five percent citing a cyberattack as their number one

66 "Terrorism Preparedness," The American Red Cross, accessed June 20, 2025, https://www.redcross.org/get-help/how-to-prepare-for-emergencies/types-of-emergencies/terrorism.html.
67 "How FEMA Works," Federal Emergency Management Agency, accessed April 10, 2025, https://www.fema.gov/about/how-fema-works.
68 "How FEMA Works."
69 See, for example: "Hurricane Katrina: Better Plans and Exercises Need to Guide the Military's Response to Catastrophic Natural Disasters," Government Accountability Office, May 25, 2006. https://www.gao.gov/products/gao-06-808t; "Hurricane Katrina: 10 Years After the Storm," Government Accountability Office, August 27, 2015, https://www.gao.gov/blog/2015/08/27/hurricane-katrina-10-years-after-the-storm; "Emergency Management: FEMA Has Made Progress, but Challenges and Future Risks Highlight Imperative for Further Improvements, Government Accountability Office, June 25, 2019. https://www.gao.gov/products/gao-19-617t.
70 "National Household Survey," Federal Emergency Management Agency, accessed April 17, 2025, https://www.fema.gov/about/openfema/data-sets/national-household-survey.
71 "2024 National Household Survey on Disaster Preparedness Findings," Federal Emergency Management Agency, accessed June 28, 2025, https://www.fema.gov/sites/default/files/documents/fema_icpd_2024-national-household-survey-on-disaster-preparedness-findings_05072025.pdf. Quote taken from p. 5.
72 "2024 National Household Survey on Disaster Preparedness Findings," 14.

concern.[73] Forty-five percent reported that they receive their disaster preparedness information from the internet, with thirty-six percent citing social media.[74]

Of significance for hybrid threats to critical infrastructure, the 2023 survey noted that "from 2019 to 2022, the five threats and hazards communities reported as most likely included cyberattacks, pandemics, floods, active shooter incidents, and earthquakes." Notably, two of these threats, cyberattacks and active shooters, are not natural disasters, and cyberattacks could include attacks against CI, although the survey did not ask this question specifically.[75]

4. Covid-19 response. The 2019–2022 Covid-19 pandemic also offers critical insights for preparing populations for the effects of major disruptions to goods and services over a prolonged period. While literature on the effects of the pandemic on the population is still unfolding, at least three key insights may help in efforts to prepare populations for hybrid attacks against CI that disrupt goods and services.

First, in the United States, the population's fears of critical goods shortages in the beginning of the pandemic led to panic-buying and hoarding items like toilet paper and medicine, which some experts believe actually created these shortages.[76] As with the Colonial Pipeline attack, panic buying and hoarding appear to be perennial challenges for the United States in the face of disruptions to goods and services caused by a range of crises. To reduce these tendencies, one team of psychiatrists advocate for governments to "implement educational programs to increase people's ability to tolerate distress and uncertainty."[77] This suggestion aligns with efforts to prepare populations for hybrid attacks as a means of minimizing their panic and overreaction.

Second, the government's efforts to inform the population about the pandemic and what to do were challenged by dis- and mal-information and conspiracy theories concerning the virus and how to prevent its spread. Significantly, one report on effective government messaging during the pandemic found a high correlation between a population's level of trust toward its government and compliance with instructions; the higher the level of trust between the population and the government, the more compliant the population was with the government's instructions. Put another way, a population's trust in its government *before* the pandemic determined how they responded to government information and instructions during the crisis.[78]

Third, populations around the world were unprepared for the psychological impact of prolonged periods on lockdown and disruptions to school and work. Much of this research is still unfolding, especially regarding the long-term effects of lockdowns on youth, but early research suggests that the psychological effects of the pandemic and the lockdown have had lasting negative effects on the population.[79] These findings may be significant for future crises that require populations to stay indoors and isolated from one another for prolonged

73 "2024 National Household Survey on Disaster Preparedness Findings," 17.

74 "2024 National Household Survey on Disaster Preparedness Findings," 20.

75 "National Preparedness Report (Based on data from 2022)," Federal Emergency Management Agency, December 2023, accessed April 18, 2025, https://www.fema.gov/sites/default/files/documents/fema_2023-npr.pdf.

76 See, for example: Andrew Moore, "How the Covid 19 Pandemic Created a Toilet Paper Shortage," *College of Natural Resource News at NC State*, May 19, 2020, https://cnr.ncsu.edu/news/2020/05/coronavirus-toilet-paper-shortage/.

77 David, Visvalingam, and Norberg provide a useful discussion on the difference between panic buying, which is based on perceived scarcity, and hoarding, which is driven by fear of uncertainty. See: Jonathan David, Shanara Visvalingam, Melissa M. Norberg, "Why Did All the Toilet Paper Disappear? Distinguishing Between Panic Buying and Hoarding During COVID-19," *Psychiatry Research* 303, no. 114062 (2022): 1–10.

78 Han, et al, used survey data from 23 countries regarding government messaging and population compliance. Their study revealed this correlation. See: Qing Han, et al, "Trust in Government Regarding COVID-19 and its Associations with Preventive Health Behaviour and Prosocial Behaviour During the Pandemic: A Cross-sectional and Longitudinal Study," *Psychological Medicine* 26 (2021), 1–11.

79 G. Sarafini, et al, "The Psychological Impact of COVID-19 on the Mental Health in the General Population," *QJM: An International Journal of Medicine* 113, no 8 (2020), 529–535.

periods, including, for example, an attack on chemical or nuclear facilities that releases contaminates and requires populations to stay indoors.

Key Takeaways:

- Societal resilience describes the ability "to resist, absorb, accommodate to and recover from the effects of a hazard in a timely and efficient manner." De Coning defines "civilian resilience" as "the ability of a society to prevent, manage and recover from hybrid attacks without losing its essential values, cohesion and identity." De Coning's definition identifies the key targets of hybrid attacks, specifically a country's values and identity, underscoring what governments and societies need to defend.
- U.S. disaster preparedness and societal resilience building, including for a nuclear attack during the Cold War, for a massive terrorist incident following 9/11, against natural disasters, and the response to the Covid-19 pandemic, suggest that preparing populations for disruptions to goods and services goes beyond providing a list of what to have on hand in the event of a crisis; disaster preparedness and societal resilience building also needs to include how to psychologically prepare for uncertainty and disruptions.
- Preparing the population and building societal resilience ahead of crises is key, especially to reduce counterproductive behavior and to return society to normal as quickly as possible.
- Lessons from the Covid-19 pandemic suggest that the degree of trust between the population and the government is positively correlated with its willingness to follow the government's instructions. In other words, the more the population trusts the government, the more likely it will follow its instructions and, conversely, the less the population trusts the government, the less likely it will follow instructions. Countries that have deep political divisions and/or a low level of trust between the government and segments of the population may struggle with physically and psychologically preparing their nation for disasters.

Some of our European allies already have programs aimed at building societal resilience to withstand hybrid threats. The next section will look at plans created by Sweden, the United Kingdom (UK), and Romania to further gain insights into best practices at building societal resilience to withstand attacks on CI and disruptions to goods and services.

3. Case Studies in Europe: Sweden, the UK, and Romania

Europe has a longstanding tradition of civil preparedness for war. During World Wars I and II, several countries took measures to prepare their populations for aerial bombardment and other activities that affected populated areas. The now ubiquitous "Keep Calm and Carry On" poster was one example the British government's efforts to prepare its population for war and to raise morale during World War II.[80] The threat of both invasion and nuclear war after World War II created a new urgency for civil defense on both sides of the Iron Curtain. Most European countries adopted some form of civil preparedness during the Cold War and NATO required civil defense as part of Article 3 of its Treaty.[81]

With the collapse of the Soviet Union in 1991, many European countries ended or greatly reduced their civil preparedness programs as part of the "peace dividend" that came with the end of the Cold War, including Sweden, a country known for its Total Defence concept.[82] However, following Russia's illegal annexation of Ukrainian territory in 2014, the EU, NATO, and individual European countries began to rebuild civil defense programs in response to a revisionist Russia.

This section outlines steps taken in Europe to build societal resilience as a means of preparing populations for a range of threats, including hybrid attacks. In addition to providing an overview of **NATO and EU efforts**, it looks specifically at efforts in **Sweden, the UK, and Romania** to build societal resilience and prepare populations for disruptions of goods and services caused by hybrid attacks on CI.

Taken together, these case studies offer different approaches to building societal resilience based on each country's history, geography, capabilities, preparedness, resources, populations, and vulnerabilities, and how NATO and the EU aim to establish baseline requirements for preparedness that transect state borders.

NATO and EU Efforts to Build Resilience

Russia's illegal annexation of Crimea and military occupation of Ukraine's eastern oblasts in 2014 prompted NATO, the EU, and individual countries to rethink their defense programs, including civil preparedness. In addition to calling Russia's activities "a violation of Ukraine's sovereignty and territorial integrity," then NATO Secretary-General Anders Fogh Rasmussen declared, "This is a wake-up call for the Euro-Atlantic community, for NATO, and for all those committed to a Europe whole, free and at peace."[83]

Following Russia's illegal actions in Ukraine, NATO held a summit in Wales in September 2014. The member states issued "The Wales Summit Declaration" and the "Joint Statement of the NATO-Ukraine Commission,"

80 Interestingly, the poster was not widely distributed during the war. See Stuart Hughes, "The Greatest Motivational Poster Ever?" *BBC*, February 4, 2009, accessed May 3, 2025, http://news.bbc.co.uk/2/hi/uk_news/magazine/7869458.stm.

81 Article 3 of the Treaty states, "In order more effectively to achieve the objectives of this Treaty, 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." See: "Resilience, Civil Preparedness and Article 3," North Atlantic Treaty Organization, accessed May 12, 2025, https://www.nato.int/cps/en/natohq/topics_132722.htm.

82 Eric Adamson and Jason Moyer, "In From the Cold: Rebuilding Sweden's Civil Defense for the NATO Era," *War on the Rocks*, April 9, 2024. https://warontherocks.com/2024/04/in-from-the-cold-rebuilding-swedens-civil-defense-for-the-nato-era/.

83 Fred Dews, "NATO Secretary General: Russia's Annexation of Crimea is Illegal Illegitimate," Brookings, March 19, 2014, https://www.brookings.edu/articles/nato-secretary-general-russias-annexation-of-crimea-is-illegal-and-illegitimate/.

which vigorously condemned Russia's disregard for international law and called for its immediate withdrawal from Ukrainian territory.[84] NATO members agreed to more aggressively pursue committing two percent of their gross domestic product (GDP) on defense. The Declaration also specifically called out hybrid war and hybrid threats as activities that required more than traditional military capabilities to counter, including "enhancing strategic communications, developing exercise scenarios in light of hybrid threats, and strengthening coordination between NATO and other organisations, in line with relevant decisions taken, with a view to improving information sharing, political consultations, and staff-to-staff coordination."[85]

After the summit in Wales, NATO began developing capabilities specifically designed to address hybrid threats. It opened the NATO StratCom Center of Excellence in Riga, Latvia, in 2014. In 2016, at its summit in Warsaw, NATO created the "Seven Baseline Requirements" for civil preparedness to bolster Article 3 of the NATO Treaty. NATO leadership called for these changes based on "the recognition that the strategic environment has changed, and that the resilience of civil structures, resources and services is the first line of defence for today's modern societies."[86] The Seven Baseline Requirements aimed to address deficiencies in societal resilience revealed by the mass migration crisis of 2015, several high-profile cyberattacks, and concerns over Russia's expansionist ambitions signaled by its occupation of Crimea and Ukraine's eastern oblasts.

With this range of threats in mind, the Seven Baseline Requirements call for a broader approach to preparedness, to include:

1. Assured **continuity of government** and critical government services: for instance, the ability to make decisions and communicate with citizens in a crisis
2. Resilient **energy supplies**: ensuring a continued supply of energy and having back-up plans to manage disruptions
3. Ability to deal effectively with the **uncontrolled movement of people** and to de-conflict these movements from NATO's military deployments
4. Resilient **food and water resources**: ensuring resilient supplies that are safe from disruption or sabotage
5. 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
6. Resilient **civil communications systems**: ensuring that telecommunications and cyber networks can function even under crisis conditions, with sufficient back-up capacity. This also includes 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 assessment of all risks to communications systems
7. 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.[87]

84 "Joint Statement of the NATO-Ukraine Commission," North Atlantic Treaty Organization, September 4, 2014, https://www.gov.uk/government/publications/nato-summit-2014-joint-statement-of-the-nato-ukraine-commission/joint-statement-of-the-nato-ukraine-commission; "Wales Summit Declaration," North Atlantic Treaty Organization, September 2014, https://web.archive.org/web/20150621015842/https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/351406/Wales_Summit_Declaration.pdf.

85 "Wales Summit Declaration."

86 Wolf-Diether Roepke and Hasit Thankey, "Resilience: The First Line of Defence," *NATO Review*, February 27, 2019, accessed April 29, 2025, https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html.

87 Roepke and Thankey, "Resilience: The First Line of Defence."

Notably, these baseline requirements include the four "critical lifeline" sectors of water, electricity, transportation, and communication, in addition to providing continuity of government with the overarching goal of ensuring delivery of goods and services and maintaining security.

In the wake of Russia's full-scale invasion of Ukraine in 2022, Edward Hunter Christie and Kristine Berzina proposed that NATO's baseline requirements should be expanded to include three additional pillars: payment systems, psychological resilience, and data protection. They further argue that psychological resilience requires further consideration, including "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."[88] They further assert that,

> *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…*[89]

Christie and Berzina's call for a psychological pillar of the NATO baseline requirements emphasizes that populations are the target of hybrid threats and governments need to prepare their populations to understand and defend against these threats as a matter of military preparedness for the alliance.

In 2017, the European Centre of Excellence for Countering Hybrid Threats (Hybrid COE) was founded in Helsinki, Finland, as an initiative for NATO, EU, and other partner nations to work together on understanding and withstanding hybrid threats.[90] To this end, Hybrid COE has provided a working definition of hybrid threats, what it calls a "concept," which

> *…refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronized and deliberately target democratic states' and institutions' vulnerabilities. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution.*[91]

Hybrid COE also has developed several lines of effort for understanding and countering hybrid threats, including challenges posed to societal resilience, which it defines as "threats, which exploit societal divisions, erode trust in institutions, and challenge military readiness," and which "requires a whole-of-society approach [to counter]. This entails preventive efforts among different sectors of society, combining military and civilian capabilities to strengthen resilience against hybrid threats."[92] In 2024, Hybrid COE welcomed its thirty-sixth participating country, Albania.[93]

Simultaneous to NATO efforts, the EU began to prepare its member states for hybrid threats. G. Alexander

88 Edward Hunter Christie and Kristine Berzina, "NATO and Societal Resilience: All Hands on Deck in an Age of War," *The German Marshall Fund of the United States Policy Brief,* July 2022, https://www.gmfus.org/sites/default/files/2022-07/NATO%20and%20Societal%20Resilience%20All%20Hands%20on%20Deck%20in%20an%20Age%20of%20War.pdf.

89 Christie and Berzina, "NATO and Societal Resilience: All Hands on Deck in an Age of War," 8.

90 Niklas Nilssen, et al., "Security Challenges in the Grey Zone," in *Hybrid Warfare: Security and Asymmetric Conflicts in International Relations,* eds. Mikael Weissmann, et al. (I.B. Tarus, 2021), 6.

91 Hybrid COE, "Hybrid threats as a concept."

92 "Deterrence and Resilience," Hybrid COE, accessed May 4, 2025, https://www.hybridcoe.fi/deterrence-and-resilience/.

93 "Establishment," Hybrid COE, accessed May 10, 2025, https://www.hybridcoe.fi/establishment/#:~:text=Hybrid%20CoE%20was%20officially%20established,Board%20held%20its%20first%20meeting.

Crowther argues that, following Russia's 2014 illegal annexation of Ukrainian territory, the EU took the lead for malign activities below the threshold of armed conflict within the EU, including hybrid threats, and NATO took the lead for kinetic activities.[94] In 2015, the European Union's Emergency Action Services (EEAS) created the East StratCom Task Force with the aim of explaining EU policies and supporting Eastern European countries.[95] In 2016, the Security Commission of the EU, together with the High Representative of the Union for Foreign Affairs and Security Policy, began constructing a series of products and initiatives aimed at addressing hybrid threats, including a "Joint Framework on Countering Hybrid Threats," a "Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats," and annual reports chronicling hybrid threats and progress in countering these activities.[96] In 2019, the EU adopted "The European Council Conclusions," which includes "the possibility for the Member States to invoke the Solidarity Clause (Article 222 TFEU) in addressing a severe crisis resulting from hybrid activity."[97]

The EU has taken a broad approach to resilience building as a means of defending against hybrid threats, including encouraging member states to improve resilience through legal frameworks and institutional capacity building; by building physical resilience, including reinforcing CI; by addressing dis- and mal-information; and by building societal resilience.[98] In January 2023, the EU passed the "Directive on the Resilience of Critical Entities," which aims to bring all EU member countries into compliance with standards for assessing and protecting CI across eleven sectors: "energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, space, production, processing and distribution of food."[99]

In March 2025, the EU stepped up its planning for disaster preparedness as a form of resilience building against both natural and manmade disasters. Hadja Labib, the European Commission for Humanitarian Aid and Crisis Management, released a social media clip titled, "What's in My Bag: Survival Edition," which provided a somewhat comical look at what to include in a seventy-two-hour emergency bag to prepare citizens for disruptions to critical goods and services. Her kit included water, food, a portable light source, medication, her glasses, key documents, a Swiss Army Knife, cash, radio, a power charger for a mobile phone, and playing cards.[100] This clip was picked up by media throughout the EU, with at least one far-right member of the European Parliament accusing the Commission of "war hysteria" and "creating panic."[101]

Within a month of the EU's call for all citizens to have seventy-two hours of emergency provisions, Spain and Portugal experienced an unprecedented power outage on April 28, 2025. The blackout and brief disruption to cellphone services, which are not believed to be the result of a hybrid attack, affected an estimated fifty-five

94 G. Alexander Crowther, "NATO and Hybrid Warfare: Seeking a Concept to Describe the Challenge from Russia," in *Hybrid Warfare: Security and Asymmetric Conflicts in International Relations*, eds. Mikael Weissmann, et al. (I.B. Tarus, 2021), 21–35.

95 Niklas Nilssen, et al. "Security Challenges in the Grey Zone," 6.

96 "Hybrid Threats," European Commission, accessed May 4, 2025, https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en.

97 As quoted in Sandra Kalniete and Tomass Pildegovičs, "Strengthening the EU's Resilience to Hybrid Threats," *European View* 20, No. 1 (2021), 26.

98 "Hybrid Threats," European Commission, accessed May 10, 2025, https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en.

99 "Critical Infrastructure Resilience at EU-Level," European Commission, September 23, 2024, accessed May 10, 2025, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en.

100 "What's in My Bag: Survival Edition," European Commission, accessed March 27, 2025, https://www.youtube.com/shorts/A5rCEb16yTY.

101 Amandine Hess and Romane Armangau, "The EU Commission' Survival Kits—Fearmongering or Necessary Preparedness?" *EuroNews*, April 2, 2025, https://www.euronews.com/my-europe/2025/04/02/the-eu-commissions-survival-kits-fearmongering-or-necessary-preparedness.

million people. The outage only lasted around ten hours for most affected areas but caused mass panic and public outrage, suggesting that these European citizens were, in fact, not ready for disruptions to goods and services, irrespective of whether they were caused by hybrid attacks or not.[102]

Finally, the EU and NATO have created joint efforts to build resiliency, including addressing vulnerabilities posed by hybrid attacks on CI. In January 2023, the EU and NATO issued the Joint Declaration on EU-NATO Cooperation, followed by the "Alliance Resilience Objectives at the Vilnius Summit," which aimed "to prepare the Alliance for 'strategic shocks and disruptions.'"[103] And in January 2023, the EU-NATO Task Force on Resilience of Critical Infrastructure was created to "bridge gaps between military, intelligence and law-enforcement communities, sharing best practices and enhancing situational awareness."[104] As with many of these other initiatives, it is too soon to evaluate the efficacy of these joint EU-NATO efforts to prepare and defend against hybrid attacks against CI.

In addition to NATO and EU efforts to build societal resilience and prepare populations for disruptions of goods and services, countries have also created individual plans that may provide insights on how to better build societal resilience and prepare populations for disruptions to goods and services from hybrid attacks. These countries, Sweden, the UK and Romania, have all taken measures aimed at preparing populations for hybrid threats, with differing approaches and to differing degrees.

Sweden, UK, and Romania Resilience Building

Sweden, the UK, and Romania each have taken different approaches to developing resilience programs. Sweden's concept of Total Defence builds on over eighty years of experience and is organized through its government; Romania's resilience program includes government, civil society, and private initiatives; and efforts to build resilience in the UK include an independent organization, the National Preparedness Commission (NPC), which strives to be "non-political" in its efforts to prepare people for crises. Each country also provides variation in histories, geography, capabilities, preparedness, resources, and populations, which offers a wide variety of challenges from which to learn.

Focusing on these European countries to investigate how to build societal resilience broadly and, more specifically, how to prepare populations for disruptions to critical goods and services caused by hybrid attacks to CI should reveal insights into the following questions:

- How do these countries **define critical infrastructure**? What is included, what is not, and why?
- What are the **types of hybrid attacks** that these countries have had on their critical infrastructure? How have these attacks disrupted goods and services?
- How do these countries **prepare their populations for hybrid threats** and disruptions to goods and services caused by attacks on CI, if at all? Who is responsible for education (national government agency, local, public-private, etc.)? What role does the media play in educating the population?

102 Helena Horton, "What Caused the Blackout in Spain and Portugal and Did Renewable Energy Play a Part?" *Guardian*, April 29, 2005. https://www.theguardian.com/environment/2025/apr/29/what-caused-the-blackout-in-spain-and-portugal-and-did-renewable-energy-play-a-part. See also: Chris Kremidas-Courtney, "Grid Resilience 2.0: Lessons from the Iberian Blackout," Euro-Atlantic Resilience Centre, May 2025. https://e-arc.ro/en/2025/05/26/grid-resilience-2-0-lessons-from-the-iberian-blackout-2/.

103 Charlie Edwards and Nate Seidenstein, "The Scale of Russian Sabotage Operations Against European Critical Infrastructure," International Institute for Strategic Studies, August 2025, 12, https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/.

104 Edwards and Seidenstein, "The Scale of Russian Sabotage Operations Against European Critical Infrastructure."

- What role, if any, do the **private or non-governmental sectors** play in helping populations understand, prepare for, and cope with hybrid attacks that target CI?

1. Sweden

Several factors make Sweden an important country to study in its efforts to build societal resilience.

First, given its proximity to Russia, Sweden has a longstanding tradition of preparing its entire population for the possibility of invasion and war. It pioneered the concept of "Total Defence," which is "the range of activities required to prepare Sweden for war," and "involves the whole of society."[105] Total Defence provides insights into how to build and maintain societal resilience as part of a wider defense strategy and is the model from which other countries have built their own comprehensive defense programs, including Finland.[106]

Second, Sweden underwent rapid growth in the post-Cold War era due to immigration, which has created a multicultural society that has required not only social integration, but integration into the Total Defence concept as well.[107] How Sweden has built Total Defence in its multicultural society may be useful to other multicultural nations.

Finally, as a neutral country until 2024, Sweden's mindset has been one of "going it alone" or "self-sufficiency," which required it to prepare for war without the collective defensive guarantee of Article 5 of the NATO Treaty or its nuclear umbrella. Now that Sweden has joined NATO, it must align its Total Defence with Article 3 of the Treaty and NATO's Seven Baseline Requirements. How Sweden is working toward these goals as part of its defense strategy could provide insights into how other countries could develop and improve their own resilience programs.

Sweden's Total Defence concept was created during World War II and expanded throughout the Cold War as a means of defending the kingdom from Soviet invasion. Total Defence was built on several core principles, including that the Swedish government was prepared to defend its people and territory in the event of war, that everyone in Sweden had a role to play in its country's defense, and that Swedes should never capitulate: "If Sweden is attacked by another country, we will never give up. All information to the effect that resistance is to cease is false."[108] Swedish citizens are, in fact, constitutionally obligated to fight and defend the nation, a principle is also known as "the will to defend" (*viljan att försvara*).[109]

During the Cold War, Sweden's Total Defence was built on four pillars: military, civilian, psychological, and economic defense.[110] Each of these pillars underwent detailed study and development throughout this time. The economic component, for example, had a specific list of private companies called "K companies" that were obligated to produce goods for national defense in the event of invasion or war.[111] The civil and psychological

105 "Total Defence," Government Offices of Sweden, accessed May 29, 2025, https://www.government.se/government-policy/total-defence.

106 Karl Lallerstedt, "Rebuilding Total Defense in a Globalized Deregulated Economy: The Case of Sweden," *Prism* 9, no. 23 (2021), 93

107 Lallerstedt, "Rebuilding Total Defense in a Globalized Deregulated Economy."

108 Alex Maxia, "Nordic Neighbours Release New Advice on Surviving War," *BBC*, November 18, 2024. https://www.bbc.com/news/articles/cjr4zwj2lgdo.

109 Teemu Häkkinen and Miina Kaarkoski, "Willingness to Defend and Foreign Policy in Sweden and Finland from the Early Cold War Period to the 2010s," *Scandinavian Journal of History* 49, No. 2 (2024): 266–285.

110 Fredrik Bertilsson, "The Swedish Defence Research Establishment (FOA) and the Influence of Historical Knowledge on Swedish Civil Resistance Policy," *Scandinavian Journal of History* 46, no. 4 (2021): 550–569.

111 Pär Malmberg, Jan Ottosson, Martin Eriksson, Olle Jansson, "The Role of Industry Sweden's Total Defence: Past, Present,

pillars also underwent considerable study, especially through the research of behavioral scientist Adam Roberts in the 1980s, who worked on preparing populations for resistance to invasion and occupation.[112]

One way in which the Swedish government prepared its population for war was by developing and distributing a booklet that provided guidance on what to do in the event of war or invasion. The original version, titled "If War Comes," was developed during World War II and then updated throughout the Cold War. The booklet included descriptions of critical supplies to have on hand, basic first aid, how to address psychological stresses, how to speak to children about war, where to go in the event of an air raid, the meaning of different sirens, and emergency contacts. Copies were sent out to all Swedish Citizens in 1943, 1952, 1961, and a version was included in the back of the phone book.[113]

At the end of the Cold War, Sweden's Total Defence concept was greatly reduced as part of the post-Cold War peace dividend.[114]

Several factors led to Sweden's recent efforts to rapidly rebuild its Total Defence program. First, following Russia's illegal annexation of Ukrainian territory in 2014, Sweden, along with most of Europe, began revamping its defense plan to address a resurgent Russia. Although not part of NATO at the time, Sweden's rebuilding of its Total Defence mirrored NATO efforts to bolster its defenses across the alliance after 2014. To this end, Sweden passed a defense bill in 2015 that aimed to revitalize its security posture, including its Total Defence program.[115]

A second major "wakeup call" for Sweden was the Covid-19 pandemic. The pandemic revealed that Sweden was lacking critical stockpiles of medical supplies, including personal protective equipment, and was vulnerable to international supply chain disruptions, as were most countries in the region and even the world.[116] The Finnish Institute for International Affairs (FIIA) claimed that the pandemic was a wakeup call for all the Nordic countries: "The Covid-19 pandemic demonstrated the fragility of many of the critical flows on which the Nordics depend for their security of supply."[117] The Covid-19 pandemic, in other words, revealed critical vulnerabilities that could be exploited by an adversary.

A third issue influencing Sweden's reboot of its Total Defence has been its growing multiculturalism and how it may have affected its civil defense. Social scientist Fredrik Bertilsson notes that a core component of Swedish Total Defence during the Cold War was that it was "underpinned by a fundamental belief in the social infrastructure, that loyalty and friendship were crucial to the defence and security of the country."[118] Sweden's rapid influx of immigrants following the end of the Cold War has challenged its traditional social infrastructure and therefore may be a vulnerability for its Total Defence. Moreover, Karl Lallerstedt notes that large ethnic communities, particularly Russians, Chinese, Iranians, and Syrians, may be vulnerable to foreign influence. Extremism and organized crime are also domestic security concerns in Sweden, further complicating and

---

and Future," The Royal Swedish Academy of War Sciences, September 26, 2023. https://kkrva.se/the-role-of-industry-in-swedens-total-defence-past-present-and-future/.

112 Bertilsson, "The Swedish Defence Research Establishment (FOA)."

113 "Download or order the brochure In Case of Crisis or War," Swedish Civil Contingencies Agency (MSB), accessed May 30, 2025, https://www.msb.se/en/advice-for-individuals/the-brochure-in-case-of-crisis-or-war/download-and-order-the-brochure-in-case-of-crisis-or-war/.

114 Lallerstedt, "Rebuilding Total Defense in a Globalized Deregulated Economy."

115 Pär Malmberg, et al., "The Role of Industry in Sweden's Total Defence: Past, Present, and Future."

116 Lallerstedt, "Rebuilding Total Defense in a Globalized Deregulated Economy." See also: Wigell, et al, "Nordic Resilience: Strengthening Cooperation on Security of Supply and Crisis Preparedness," 11.

117 Wigell, et al, "Nordic Resilience: Strengthening Cooperation on Security of Supply and Crisis Preparedness," 11.

118 Bertilsson, "The Swedish Defence Research Establishment (FOA)," 553.

potentially weakening civil defense.[119]

With these challenges in mind, Sweden began to rebuild its Total Defence capabilities and test them in practice. Rather than four pillars, as was the case during the Cold War, Sweden's Total Defence structure is now broadly divided into two components, military and civil defense (which also covers disaster preparedness), with separate ministers for each but with both components falling under the ministry of defense.[120]

In 2016, Sweden created what it calls "an action plan" for "protection of vital societal functions (VSF) and critical infrastructure." Rather than specifically name CI sectors, Sweden's action plan focuses on a functional definition of CI and its relationship to society, stating that CI is anything which "A loss of or a severe disruption to the activity that alone or together with other similar events, rapidly leads to a serious societal emergency or crisis."[121] In other words, Sweden's approach to protecting CI focuses on the nexus between CI and how they support various societal functions.

In 2017, Sweden held a military exercise, Aurora 17, which included all its armed forces along with civilian organizations to test its Total Defence capabilities and its interoperability with neighboring countries, the United States, France, and NATO forces, despite being a nonaligned power at the time.[122] Mike Winnerstig of the Estonian think tank International Centre for Defence and Security noted that the exercise received considerable attention from the Swedish public. "In general," he summarized, "the Swedish public seems both to accept and enjoy the fact that the Swedish armed forces are able once again to demonstrate the military capacity, at least in an exercise, that was once standard for the country. International involvement in the exercise has also been widely appreciated, especially by the Swedish troops but also, as far as can be seen, by the vast majority of the Swedish public."[123]

In 2018, the Swedish government reissued its civil preparedness booklet to its entire population, now called *In Case of Crisis or War*, and updated it again in 2024 to reflect Sweden's inclusion in the NATO alliance.[124] The booklet begins by stating,

> *We live in uncertain times. Armed conflicts are currently being waged in our corner of the world. Terrorism, cyber attacks, and disinformation campaigns are being used to undermine and influence us.*
>
> *To resist these threats, we must stand united. If Sweden is attacked, everyone must do their part to defend Sweden's independence – and our democracy.*
> *We build resilience every day, together with our loved ones, colleagues, friends, and neighbours.*
>
> *In this brochure, you learn how to prepare for, and act, in case of crisis or war.*
> *You are part of Sweden's overall emergency preparedness.*[125]

119 Lallerstadt, "Rebuilding Total Defense in a Globalized Deregulated Economy," 99.
120 "Total Defence," Government Offices of Sweden, accessed May 30, 2025, https://www.government.se/government-policy/total-defence.
121 "Protection of Vital Societal Functions & Critical Infrastructure," Swedish Civil Contingencies Agency (MSB), August 2016. https://www.msb.se/siteassets/dokument/publikationer/english-publications/protection-of-vital-societal-functions--critical-infrastructure.pdf.
122 Justyna Golkowska, "Aurora: Sweden's Response to Zapad?" OSW: Center for Eastern Studies, September 20, 2017, https://www.osw.waw.pl/en/publikacje/analyses/2017-09-20/aurora-swedens-response-to-zapad#:~:text=The%20Aurora%2017%20national%20military,military%20exercise%20in%20recent%20years.
123 Mike Winnerstig, "The Strategic Ramifications of the Aurora 17 Exercise in Sweden," International Centre for Defence and Security, October 2, 2017, https://icds.ee/en/the-strategic-ramifications-of-the-aurora-17-exercise-in-sweden/.
124 "Download or order the brochure In Case of Crisis or War."
125 "In Case of Crisis or War," 3.

The booklet is available in Swedish, "simple" or "light" Swedish, and English.[126]

A Google search for the brochure shows that the 2024 manual has been reposted in a number of countries, including Germany, Italy, and the United States, suggesting that it has become a useful document for other countries creating their own civil defense programs. Also around this time, Finland, Norway, and Denmark made similar efforts to instruct their populations to prepare for the possibility of disruptions to goods and services and the need to go it alone for a period of time.[127]

Following Russia's full-scale invasion of Ukraine in 2022, Sweden created the Psychological Defence Agency as a separate government entity. Its mission "covers external information influence that is directed at Sweden with the aim of harming Swedish interests. The purpose of psychological defence is to safeguard freedom of expression and open and democratic society."[128] The Psychological Defence Agency has three departments—administration, capabilities, and operations—which work to defend Sweden from dis- and mal-information and prepare government, law enforcement, and society to identify and defend against malign psychological influences.[129]

In January 2024, following elections and a new administration in Sweden, Carl Oskar Bohlin, Sweden's Minister for Civil Defence, spoke at an annual security conference in Sälen. Within the context of Russia's growing revanchism, he unequivocally stated, "There could be war in Sweden." He went on to say,

> *Societal resilience requires…situational awareness. Awareness among individual citizens, employees, entrepreneurs and decision-makers in public administration. But it is not enough to simply contemplate the question. Civil defence is not primarily a theoretical exercise. Awareness must be translated into practical action.*[130]

The speech, which was broadcast in Sweden, caused alarm and debate throughout the country and beyond. The former Prime Minister of Sweden, Magdalena Andersson, argued that "it is not as if war is just outside the door,"[131] and one journalist called Bohlin's words "the militarization of our conscience."[132] Sweden joined NATO shortly after this speech, on March 7, 2024.

In another effort to inform and prepare Swedes for hybrid threats and war, the *Försvarsmakten*, the Swedish Defense Forces, released a six-part series on YouTube in October 2024 called "*Krig i Vår Tid*," (War in Our Time), which outlines the current security threat to Sweden and the need for a whole-of-society, Total Defence response. The episodes have self-explanatory titles: "A Dark Future," "The Extremity of War," "Know Your Enemy," "One Is Not Strong," "The Fragile Society," and "Team Sweden," and take the viewer through the threat posed primarily by Russia, how the Swedish government and military are responding, and the need

126 "Download or order the brochure In Case of Crisis or War."
127 Maxia, "Nordic Neighbours Release New Advice on Surviving War."
128 "Our mission," Psychological Defence Agency (Government of Sweden).
129 "Our organizations," Psychological Defence Agency (Government of Sweden), accessed July 7, 2025, https://mpf.se/psychological-defence-agency/about-us/our-mission/organisation.
130 "Speech by Minister for Civil Defence Carl-Oskar Bohlin at Folk och Försvars Annual National Conference in Sälen on the 7th of January 2024," Government Offices of Sweden, https://www.government.se/speeches/2024/01/speech-by-minister-for-civil-defence-carl-oskar-bohlin-at-folk-och-forsvars-annual-national-conference-in-salen-on-the-7th-of-january-2024/.
131 Paul Kirby, "Swedish Alarm after Defence Chiefs' War Warning," *BBC*, January 10, 2024. https://www.bbc.com/news/world-europe-67935464.
132 Göran Greider, "Micael Bydén Cannot, of Course, Say Out Loud That He Longs for War," *Dagens Nyhetter,* January 8, 2024, https://www.dn.se/kultur/goran-greider-micael-byden-kan-naturligtvis-inte-saga-hogt-att-han-langtar-efter-krig.

for unity and for all Swedes to prepare to defend their country.[133] Of note, several vloggers have watched the episodes and commented on the series, including U.S. and British soldiers. [134]

In December 2024, Sweden passed the Total Defence Bill 2025–2030, which aims to update preparedness, including informing populations about hybrid threats, and messaging in times of crisis.[135] In January 2025, Bohlin again addressed the country's annual security conference about Total Defence:

> *Let me be just as clear as I was last year when I said that war could also come to our doorstep. The age of extreme individualism is over. The future will demand greater unity. Protecting Sweden's interests is a greater task than our own self-realisation… ultimately, it is about a joint commitment to the defence of our society, democracy and values. The essence of total defence is that the defence of our country is not a task for a few, but a task for all of us.*[136]

And on May 16, 2025, Sweden signed a Memorandum of Understanding (MOU) with Norway, Iceland, and "Baltic Sea countries within the EU" concerning the protection of CI in the Baltic Sea. This MOU was in response to increasing damage to underseas cables in the Baltic Sea, and the strong suspicion that these incidents may be hybrid attacks perpetrated by Russia. The MOU aims "to strengthen regional cooperation through increased information sharing, improved situational awareness and the exchange of best practices and measures. It also encompasses cooperation within the frameworks of the EU, NATO and other organisations."[137]

Finally, alongside these unilateral efforts to build Total Defence, Sweden, together with Finland, Norway, and Denmark, is working toward a regional approach to defense, which puts societal resilience at its core. A FIIA report notes,

> *In all the Nordics, the adoption of security concepts and practices that highlight broad or comprehensive security underpins the view that modern preparedness – comprising both military and civilian pillars – requires various societal actors, ranging from government to business and civil society organisations, to build resilience capacities, support the state in maintaining preparedness and ensure the continuity of vital societal functions.*[138]

The report further notes that,

> *All the Nordics promote an all-hazards approach to preparedness, which targets the full spectrum of threats in preparedness planning, regardless of their source, causality or likelihood. In other words, all the Nordics use a preparedness approach that aims at building capacities and capabilities to manage crises, disasters and disruptions, whether they are the result of man-made, natural, technological or societal hazards.* [139]

---

133 "War in Our Time," Försvarsmakten (YouTube), accessed June 1, 2025, https://www.youtube.com/playlist?list=PLGXVHgImhBQI4-E55p7q8ngE_-L-GuK3g.

134 See, for example, "Sweden – War in Our Time Episode 1/6: A Dark Future (US Soldier Reacts) Krig I Var Tid, Just Another Army Vet (YouTube), accessed June 1, 2025, https://www.youtube.com/watch?v=5ySShpkfIrc.

135 "Total Defence," Government Offices of Sweden, accessed February 1, 2025, https://www.government.se/government-policy/total-defence/.

136 "Speech by Minister for Civil Defence Carl-Oskar Bohlin at the Folk och Försvar National Conference 2025," Government Offices of Sweden, January 17, 2025, https://www.government.se/speeches/2025/01/speech-by-minister-for-civil-defence-carl-oskar-bohlin-at-the-folk-och-forsvar-national-conference-2025/.

137 "Sweden Signs Memorandum of Understanding on the Protection of Critical Undersea Infrastructure," Government of Sweden, May 21, 2025, https://www.government.se/press-releases/2025/05/sweden-signs-memorandum-of-understanding-on-the-protection-of-critical-undersea-infrastructure/.

138 Wigell, et al, "Nordic Resilience: Strengthening Cooperation on Security of Supply and Crisis Preparedness," 11–12.

139 Wigell, et al, "Nordic Resilience: Strengthening Cooperation on Security of Supply and Crisis Preparedness," 11–12.

The report calls for a Nordic framework for resilience that moves beyond bilateral agreements to include one framework to plan, pool resources, foster public-private initiatives, and create a Nordic Resilience Fund.[140]

2. The United Kingdom

In 1996, the Irish Republican Army (IRA) hatched a plot to use explosive devices to attack power stations in the UK, with the goal of causing mass disruptions and ultimately shutting down the entire national system. British intelligence discovered the operation before the IRA could launch its attack, preventing what could have been a disastrous terrorist incident that might have caused systemic-level power outages. Journalist Rob Hastings retold this story in a 2023 article to stress that, while the IRA may no longer be a direct threat to the electrical grid, other malign actors may be targeting the UK's electrical system through cyberattacks and sabotage with the same intent of shutting down the system and causing mass panic throughout the UK.[141]

Hastings' concerns about vulnerabilities to the UK's power grid and other CI are well founded. In 2022, 2023, 2024, and 2025, the UK experienced a series of cyberattacks against CI (what it calls Critical National Infrastructure, CNI), including attacks on its electrical grid and its National Healthcare System (NHS).[142] A June 2024 cyberattack on the NHS in London, for example, postponed "over 10,000 outpatient appointments and 1,693 elective procedures… across King's College Hospital, and Guy's and St Thomas' Hospital" and prompted the drafting of a cybersecurity bill in parliament.[143]

The UK has named Russia as the principal state actor perpetrating cyber and other hybrid attacks against its CNI, claiming its activities as retaliation for Britain's support for Ukraine in the war. A 2023 report from the UK's National Cyber Security Centre (NCSC) summarized that "in cyberspace, Russia continues to be one of the world's most prolific cyber actors. It dedicates significant resources towards conducting cyber operations around the globe and poses a significant and enduring threat to the UK."[144] The report further notes,

> *Over the past 18 months we have seen a new class of Russian cyber adversary emerge. State-aligned actors (the favoured language used by the UK government to describe these groups) are often sympathetic to Russia's further invasion and are ideologically, rather than financially, motivated. They have been emboldened to act with impunity regardless of whether or not they have Russia's backing.*[145]

These attacks have included Distributed Denial of Service (DDoS) attacks, cyber espionage, the use of malware and ransomware, and may also include physical sabotage against Britain's underseas cables. In 2024, British Member of Parliament Pat McFadden warned that Russia could launch "unprovoked attacks against our critical national infrastructure" and it "can turn the lights off for millions of people."[146]

Emphasis added.

140 Wigell, et al, "Nordic Resilience: Strengthening Cooperation on Security of Supply and Crisis Preparedness,"16.

141 Rob Hastings, "The Disaster Awaiting Us if a Cyber Attack Cuts All the UK's Electricity," *The iPaper*, December 25, 2023, https://inews.co.uk/news/technology/ministers-fear-cyber-attack-cutting-electricity-2809348.

142 Dan Milmo, "Russia Can Turn the Lights Off: How the UK is Preparing for Cyberwar," *The Guardian*, 3 December 2024, https://www.theguardian.com/technology/2024/dec/03/russia-can-turn-the-lights-off-how-the-uk-is-preparing-for-cyberwar.

143 "Cyber Security and Resilience Bill," Government of the UK, accessed June 4, 2025, https://www.gov.uk/government/collections/cyber-security-and-resilience-bill.

144 "Annual Review 2023," U.K. National Cyber Security Centre, 2023, accessed June 23, 2025, https://www.ncsc.gov.uk/collection/annual-review-2023.

145 "Annual Review 2023," 18.

146 Victor Jack, "UK Warning: Russia's 'Aggressive' Cyber Warfare is Threat to NATO," *Politico*, November 24, 2024, https://www.politico.eu/article/russias-aggressive-cyberattack-putin-poses-threat-nato-uk/.

Alongside malicious state actors, accidents and natural disasters are also a concern for Britain's CNI, particularly its power grid. An accidental fire in March 2025 at an electrical station shut down Heathrow Airport for nearly a day, disrupting thousands of passengers and flights, underscoring the electrical system's vulnerability to not only attacks, but accidents as well.[147] Natural disasters also remain a persistent threat. Hastings notes, "Nature could harm us, too. Violent storms, capable of localised havoc by bringing down wires and flooding substations, are becoming more likely with climate change—and the sun could knock out our national supplies if we're hit by a solar flare of radiation that can burn out cables and substations."[148]

The UK is aware of the vulnerabilities it faces in protecting its CNI and has taken several measures to address both natural and manmade threats.

First, the government has clearly identified CNI as:

> *Those facilities, systems, sites, information, people, networks and processes, necessary for a country to function and upon which daily life depends. It also includes some functions, sites and organisations which are not critical to the maintenance of essential services, but which need protection due to the potential danger to the public (civil nuclear and chemical sites for example).*[149]

From this definition, it identifies fourteen infrastructure sectors: chemicals, civil nuclear, communications, data centres, defence, emergency services, energy, finance, food, government, health, space, transport, and water.[150]

Second, the British government has invested considerable energy into cybersecurity as a means of protecting CNI and other national vulnerabilities. In 2016, the same year the UK left the EU, it stood up the NCSC, which is part of the Government Communications Headquarters (GCHQ). The NCSC aims "to make the UK the safest place to live and work online and bring clarity and insight to an increasingly complex online world." To this end, the NCSC provides online resources for individuals and organizations of all sizes facing a range of cyberattacks; resources for managing online data; guidance for how to "retire digital assets"; a portal for reporting malign cyber activity; and annual reports, among other tools.[151]

One of NCSC's approaches to improving cybersecurity is a public-private collaborative called Cyber-Security Information Sharing Partnership (CISP), which is "a platform for cyber security professionals in the UK to collaborate on cyber threat information in a secure and confidential environment."[152] NCSC Annual Reports underscore the importance of these partnerships. "Central to our whole of society approach, the NCSC has ensured long-lasting and meaningful impact by building trust groups, industry-specific communities of Chief Information Security Officers (CISOs) in businesses and organisations. This is now an established model that sees us work in collaboration with the trust groups on raising the cyber resilience in their sectors."[153]

The UK also created a cyber strategy in 2021 with the aim of addressing current and future threats emanating from the cyber domain. "Government Cyber Security Strategy: Building a Cyber Resilient Public Sector: 2022–2030" outlines both the threat posed to Britain in the cyber domain and the government strategy of "building greater cyber resilience across all government organisations and working together to 'defend as one'—exerting

147 Simon Jack, "How Did a Single Fire Bring Down Europe's Busiest Airport?" *BBC*, March 21, 2025, https://www.bbc.com/news/articles/cdjy0g01z1po.
148 Hastings, "The Disaster Awaiting Us if a Cyber Attack Cuts all the UK's Electricity."
149 "Critical National Infrastructure," National Protective Security Authority, Government of the UK, May 23, 2025, accessed June 4, 2025, https://www.npsa.gov.uk/about-npsa/critical-national-infrastructure.
150 "Critical National Infrastructure."
151 "Homepage," The National Cyber Security Centre, accessed June 4, 2025, https://www.ncsc.gov.uk/, as of 4 June 2025.
152 "About CISP," National Cyber Security Centre, accessed June 4, 2025, https://www.ncsc.gov.uk/cisp/home.
153 "Annual Review 2023," 23.

a defensive force greater than the sum of our parts." The Strategy, in particular, notes the cyber threats posed to CI and other government resources. "Government organisations—and the functions and services they deliver—are the cornerstone of our society. It is their significance, however, that makes them an attractive target for an ever-expanding army of adversaries…Building and maintaining our cyber defences is therefore vital if we are to protect the functions and services on which we all depend."[154]

Ciaran Martin, the former head of NCSC, stressed in a 2025 interview that the private sector also has a critical role to play in ensuring that its cyber defenses are strong and that they can maintain the delivery of critical goods and services. He advised that, "Every organisation should have a plan on how to deal with the loss of a major infrastructure network. The difference between being 50% functional within 24 hours of an attack and being offline for a fortnight is huge."[155]

Third, following Russia's full-scale invasion of Ukraine in 2022 and the UK's unequivocal condemnation of the invasion and support for Ukraine, the British government drafted the "UK Government Resilience Framework," which aims to address vulnerabilities and threats across the United Kingdom. The Resilience Framework "is built around three fundamental principles: that we need a shared understanding of the risks we face; that we must focus on prevention and preparation; and that resilience requires a whole of society approach." The Framework goes on to stress, "We are committed to working with partners, industry and academia from across the UK to implement this Framework but also as we continue to develop our approach."[156]

Building off the Resiliency Framework, the UK has proposed legislation aimed at protecting its CNI from attack, including cyber legislation. In July 2024, following the cyberattack against the NHS, the Department of Science, Innovation, and Technology (DSIT) introduced the "Cyber Security and Resilience Policy Statement" along with several legislative proposals in the British Parliament with the aim of "tackling the growing cyber threat to vital services such as water, power and healthcare."[157] The "Cyber Security and Resilience Bill" was introduced in April 2025, to be heard later in the year.[158]

Also building off the Resiliency Framework, the UK government began worst-case scenario planning for disruptions to electricity and gas supplies, particularly in the winter months. In 2023, it published the "British Energy Security Strategy," and its "Net Zero Strategy.[159] Some mitigation efforts include prioritizing energy sources, reopening strategic gas reserve sites, which were closed in 2017, and creating a rolling blackout schedule.[160] Alongside an energy strategy, the UK government also published a "Supply Chain Resilience Strategy" to get ahead of potential shortfalls in critical goods, like medical supplies, which were revealed in the Covid-19 pandemic.[161]

154 "Government Cyber Security Strategy: Building a Cyber Resilient Public Sector: 2022-2030," Government of the UK, accessed June 4, 2025, https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf, 7.

155 Milmo, "Russia Can Turn the Lights Off."

156 "The UK Government Resilience Framework," Government of the UK, June 4, 2025, https://www.gov.uk/government/publications/the-uk-government-resilience-framework/the-uk-government-resilience-framework-html.

157 Jonathon Ellison, "Cyber Security and Resilience Policy Statement to Strengthen Regulation of Critical Sectors," National Cyber Security Centre, accessed June 5, 2025, https://www.ncsc.gov.uk/blog-post/cyber-security-resilience-bill-policy-statement.

158 "Policy Paper: Cyber Security and Resilience Bill: Policy Statement," Government of the UK, accessed June 5, 2025, https://www.gov.uk/government/publications/cyber-security-and-resilience-bill-policy-statement.

159 "Powering Up Britain: Energy Security Plan," Government of the UK, April 4, 2023, accessed June 5, 2025, https://www.gov.uk/government/publications/powering-up-britain/powering-up-britain-energy-security-plan.

160 Rob Hastings, "How the UK's Emergency Electricity Rationing Plans Could Work This Winter," *The iPaper*, October 8, 2022, https://inews.co.uk/news/uk-blackout-plans-government-emergency-strategy-winter-electricity-rationing-1899998?ico=in-line_link.

161 "The UK Government Resilience Framework."

Despite this impressive list of strategies, policies, and other measures taken by the UK government to defend its CNI from manmade and natural disasters, critics note that disruptions to goods and services cannot be completely prevented and that the population needs to be prepared for disruptions. For example, Jamie MacColl, an analyst at the Royal United Services Institute (RUSI), asserts that malign state actors target CNI with the aim of causing mass panic. "One of the aims of Russian activity below the threshold of war, like cyber-attacks, is to spread fear, panic and discord." Given this, he argues that "the best response to that is to be psychologically resilient and not go out into the street and buy all the toilet roll in Sainsbury's."[162]

Alongside its strategies and policies, the UK government has developed resources aimed at preparing its population for disruptions to goods and services caused by both manmade and natural disasters. As part of its resilience strategy, the government created a website called "Prepare," which includes guidance on preparing for disruptions of goods and services, and what to do in the event of a crisis.[163] The website includes a Microsoft Word document that individuals can download and fill out with critical information, including key telephone numbers, a list of prescription medications, people to contact, and items to have on hand in the event of an emergency.[164]

Beginning in April 2023, the UK began testing its emergency alert system, sending alerts through mobile devices, along with explaining to the public why the government is sending these alerts, and a schedule of future tests.[165]

Another resource is the UK government's National Emergencies Trust, which provides resources to build and maintain resilience. It "brings together the public, private and third sectors to compare perspectives and shape plans in the round to strengthen the UK's resilience" and works to receive public donations in the aftermath of a crisis.[166]

The UK Government's Cabinet Office has also created a training center for disaster preparedness and crisis management. On April 28, 2025, the government transformed the Emergency Planning College into the UK Resiliency Academy (UKRA) "to train more than 4,000 people each year, working in both public services and the private sector, to better deal with crises."[167] While the majority of instruction appears to focus on crisis management, it does include preparedness as one of its skills and identifies resilience as a "mindset," and states that it "will also provide the knowledge and tools for society to empower them to be better prepared and more resilient, signposting to helpful resources."[168]

However, perhaps the UK's greatest resource for preparing its population for major disruptions to goods and services comes from outside the government. The National Preparedness Commission (NPC) was created in 2020, in the midst of the Covid-19 crisis, as "an independent and non-political body, whose fundamental

162 Milmo, "Russia Can Turn the Lights Off."
163 "Prepare," Government of the UK, accessed June 5, 2025, https://prepare.campaign.gov.uk.
164 The document does not recommend amounts of goods to have on hand and cash is not on the list. See: "Household Emergency Plan," Government of the UK, accessed June 6, 2025, https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fprepare.campaign.gov.uk%2Fwp-content%2Fuploads%2Fsites%2F196%2F2024%2F05%2FHMG-Household_Emergency_Plan_WORD.docx&wdOrigin=BROWSELINK.
165 "Testing the Emergency Alerts Service," Government of the UK, accessed June 5, 2025, https://www.gov.uk/alerts/system-testing; "About Emergency Alerts," Government of the UK, accessed June 5, 2025, https://www.gov.uk/alerts.
166 "National Emergencies Trust," Government of the UK, accessed June 6, 2025, https://nationalemergenciestrust.org.uk/.
167 Robert Hall, "The UK Resilience Academy is Born," *Resilience Forward*, April 30, 2025. https://resilienceforward.com/the-uk-resilience-academy-is-born/.
168 "Preparedness," UK Resilience Academy, accessed June 5, 2025, https://ukresilienceacademy.org/learn/preparedness/.

objective is to promote policies and actions to help the UK be significantly better prepared to avoid, mitigate, respond to, and recover from major shocks, threats and challenges."[169] It partners with organizations from both the private and public sectors and includes "senior figures from public life, business, academia and civil society with the mission of promoting better preparedness in the UK for a major crisis or incident."[170]

The NPC website includes articles and reports on seven areas of preparedness: Disaster Response; Governance and Risk Management; Government; Policy and Legislation; Organizational Preparedness; Risk or Threat Domains; and Societal Preparedness. Its mission ranges from influencing government on disaster preparedness to informing communities and individuals on best practices in preparing for a range of crises. "Making every level of government, organisation, community, household and individual better prepared will help to ensure that the whole of UK society is better able to avoid, absorb and respond to future global crises, whether predictable—a new pandemic, a massive cyber-attack, climate change—or something genuinely unforeseen."[171]

3. Romania

On November 24, 2024, Romania held the first round of scheduled elections for a new president. Călin Georgescu, a far-right, relatively unknown candidate received the highest number of votes, raising immediate suspicions of election interference and possible fraud. Georgescu, who ran on conservative Christian values, anti-EU and NATO rhetoric, and a pro-Russian stance, had campaigned almost exclusively through social media, particularly via TikTok.[172] On December 6, Romania's Constitutional Court made the highly controversial decision to cancel the election results, citing Russian online interference through "suspicious TikTok accounts and secret payments to online influencers."[173] Elections were rescheduled for May 2025, in which the pro-EU mayor of Bucharest, Nicușor Dan, narrowly won the race.[174] Romania's challenges to its democratic processes underscore the hybrid threats it faces as a country, especially from Russia.

Romania is geographically and strategically important as an "eastern flank" country on the geographic edge of Europe. During the Cold War, Romania was a Soviet satellite state and member of the Warsaw Pact. However, it joined NATO in 2004, following the collapse of the Soviet Union. As a NATO member, Romania provides critical access to the Black Sea and hosts the largest NATO base in Europe, along with several other smaller bases.[175] Romania also joined the EU in 2007 and became part of the Schengen Zone in 2025, making it politically and economically important to Europe as well.[176]

Given its strategic importance, Romania is a likely target of a variety of Russian hybrid threats designed

169 "About," National Preparedness Commission, accessed June 6, 2025, https://nationalpreparednesscommission.uk/about/.
170 "National Preparedness Commission," LinkedIn, accessed June 6, 2025, https://www.linkedin.com/company/national-preparedness-commission/?originalSubdomain=uk.
171 "Our Mission," National Preparedness Commission, accessed June 6, 2025, https://nationalpreparednesscommission.uk/about/our-mission/.
172 Rowan Ings, "The TikTokers Accused of Triggering an Election Scandal," *BBC*, April 30, 2025, https://www.bbc.com/articles/cqx41x3gn5zo. See also: Tim Ross, "Romanian Court Cancels Presidential Elections Amid Russian Influence Fears, *Politico*, December 6, 2024, https://www.politico.eu/article/romania-court-cancels-presidential-election-runoff-tiktok-russian-influence-calin-georgescu/.
173 Ings, "The TikTokers Accused of Triggering an Election Scandal."
174 Sarah Rainsford, Paul Kirby, and Olimpia Zagnat, "Liberal Mayor Dan Beats Nationalist in Tense Race for Romanian Presidency," *BBC*, May 19, 2025, https://www.bbc.com/news/articles/crk2xxzxkzxo.
175 Madalin Necsutu, "Romania to Host Largest NATO Military Base in Europe," *Balkan Insight*, March 21, 2024, https://balkaninsight.com/2024/03/21/romania-to-host-largest-nato-military-base-in-europe/.
176 "Bulgaria and Romania Join the Schengen Area," European Commission, January 3, 2025. https://home-affairs.ec.europa.eu/news/bulgaria-and-romania-join-schengen-area-2025-01-03_en, as of 11 June 2025.

to distract or weaken its support for NATO and the EU. In addition to election interference, Romania has experienced several largescale cyberattacks attributed to Russia, including DDoS attacks on government, military, banking, and transportation websites on April 29, 2022, after Romania announced it would send aid to Ukraine. A pro-Kremlin hacking group called Killnet, which also targeted the Czech Republic, was suspected of perpetrating the attacks.[177]

In addition to cyberattacks, Romania has also had threats of physical sabotage to its CI. In January 2025, its domestic intelligence services (*Serviciul Român de Informații,* or SRI) foiled a plot by a Colombian national targeting Romania's energy CI. SRI claims that this individual was part of "an extensive network of saboteurs targeting European countries, controlled through intermediaries by the Russian secret services."[178]

In response to this amount of nefarious activity, Romania has taken several steps to protect against hybrid threats, including against its CI. First, it defines its CI largely along NATO's Seven Baseline Requirements: "the production and distribution of electricity, production and distribution of oil and gas, telecommunications, the financial system, transportation, water management, medical emergencies, and the continuity of government activities."[179] This definition covers the four "lifeline" sectors of energy, water, transportation, and communications, but also includes medical and continuity of government in line with the NATO Baseline Requirements.

Second, Romania has established a clear chain of command for protecting its CI. The Critical Infrastructure Protection Coordination Center within the Ministry of Internal Affairs is responsible for defending and protecting its CI. As an EU member state, Romania conforms to EU directives set out for CI protection, particularly Directive 2008/114/CE, which includes monitoring CI for threats, providing reports, and working with experts to ensure that its CI is secure.[180]

The Romanian Ministry of Internal Affairs also maintains the Department for Emergency Situations, which "coordinates the activities related to preventing and tackling emergency situations, to ensuring and coordinating human, material and financial resources which are necessary to restore normality after risk situations." It also coordinates emergency medical activities in the event of disasters.[181]

In 2021, the Romanian government drafted a cyber security strategy for 2022–2027. The strategy begins by outlining the threat landscape:

> *Romania is present on the map of cyberattack targets, constantly facing both complex attacks, which aim to obtain strategic advantages or financial benefits, with a potential major impact on national security, society and the economy, as well as "classic" attacks, which use common malware and exploit*

177 Madalin Necsutu, "Cyber Attacks Hit Romanian Government Websites," *Balkan Insight*, April 29, 2022. https://balkaninsight.com/2022/04/29/cyber-attacks-hit-romanian-government-websites/.
178 "SRI Foiled a Sabotage Operation Conducted by the Russian Federation on Romania's Territory," January 17,2025, https://www.sri.ro/articole/SRI-foiled-a-sabotage-operation-conducted-by-the-Russian-Federation-on-Romanias-territory.html.
179 Marius Laurentiu Rohart, "Overview of Critical Infrastructure Protection in Romania," The 9th International Scientific Conference "Defense Resource Management in the 21st Century," Braşov, Romania, November 14, 2014. https://codrm.eu/wp-content/uploads/2024/12/32_Rohart.pdf.
180 "Coordinating Centre for Protection of Critical Infrastructure," Ministry of Internal Affairs of the Government of Romania, accessed June 12, 2025, https://www.mai.gov.ro/en/coordinating-centre-for-protection-of-critical-infrastructure/.
181 "Department for Emergency Situations, Romania," Ministry of Internal Affairs of the Government of Romania, accessed June 12, 2025, https://civil-protection-knowledge-network.europa.eu/organisations/department-emergency-situations-romania.

widespread and known vulnerabilities, and which, although they have a low potential to harm national security, affect the economy and society.[182]

The cybersecurity strategy names five objectives: to create secure and resilient networks and IT systems; to strengthen regulatory and institutional frameworks; to create public-private partnerships; to develop "resilience" through proactive approaches and deterrence; and "to maintain Romania as a relevant actor in the international cooperation architecture."[183]

Outside the government, Romania has also created capabilities designed to defend against a range of hybrid threats. In 2021, Romania founded the Euro-Atlantic Resilience Centre (E-ARC) in Bucharest with backing from NATO and the EU. Its mission is "to take a whole-of-government approach to enhancing the resilience of our societies" and to be a center of excellence for societal resilience throughout Europe.[184] E-ARC produces reports, holds conferences, and maintains a network of experts across Europe to discuss various aspects of resilience. One of its initiatives is to prepare populations for crises, including disruptions of goods and services caused by both manmade and natural disasters.

In 2024, E-ARC worked with the Government of Romania to create the thirty-two-page "Guide for Crisis Situations," a guidebook for disaster preparedness, which is available in Romanian and English.[185] The guidebook stresses that the Romanian government has the capacity to care for its population and that any disruptions to critical goods and services will only be temporary.[186] It begins by asking, "How would you react if, suddenly, a natural or man-made disaster were to occur near your home and access to gas, water, electricity, banking services etc. were interrupted?"[187] The guidebook includes a scorecard for individuals to test their preparedness level, which has items like a preparedness plan, a seventy-two-hour survival kit, cash on hand, and level of involvement in one's community.[188]

The guidebook contains information on what to have on hand in case of an emergency, including food, water, medicine, cash, a whistle, and a radio, among other things.[189] It also provides basic first aid instructions, instructions for how to use a fire extinguisher, and other safety instructions, as well as how the alarm system works in Romania.[190]

In addition to what to do in a time of emergency, the guidebook includes best practices for "cyber hygiene," including creating strong passwords, backing up information, installing antivirus software, and numbers to call in the event of a cyber incident. The guidebook stresses that, "In a crisis situation, criminal groups and hostile states will attempt to take advantage of the inherent confusion and panic to steal private information or disable critical computer systems."[191]

---

182 Via Google translate, see: "Romania's Cyber Security Strategy: 2022–2027," Legislative Portal of the Government of Romania, December 30, 2021, accessed June 13, 2025, https://legislatie.just.ro/Public/DetaliiDocumentAfis/250235.
183 "Romania's Cyber Security Strategy: 2022–2027."
184 "Euro-Atlantic Resilience Centre Mission Statement," Euro-Atlantic Resilience Centre, accessed February 3, 2025, https://e-arc.ro/en/2024/03/18/e-arc-mission-statement/.
185 "Guide for Crisis Situations," Government of Romania, 2024, https://e-arc.ro/wp-content/uploads/2024/06/Guide-EN.pdf.
186 "Guide for Crisis Situations," 4, 7.
187 "Guide for Crisis Situations," 4, 7.
188 "Guide for Crisis Situations," 2–3.
189 "Guide for Crisis Situations," 14–15.
190 "Guide for Crisis Situations," 14–15, 22–23, 25.
191 "Guide for Crisis Situations," 16–17.

The guidebook also provides basic information on spotting dis- and mal-information, stressing that, "In a crisis situation, rumors and false information spread very quickly, sometimes amplified by state or non-state actors hostile to Romania with the aim of sowing panic, disrupting the intervention of the authorities and destabilizing society."[192] It also warns that people may want to take advantage of others in times of crisis, and to be on the lookout for scams and other threats.[193]

The guidebook stresses the importance of community in a time of crisis:

> *Help people around you under the direction of authorities, donate blood, volunteer, offer help or information when requested by authorities, and obey applicable laws on your own initiative! The greater the solidarity between citizens, the easier and faster we will overcome any crisis. Did you know that, according to disaster survival studies, the greater the spirit of community solidarity, the more likely group members are to survive accidents from which they could easily be saved by their peers? Identify in advance where you can volunteer or get directly involved to help members of your community! You too might one day need help from your peers! Help the people around you![194]*

The guidebook even offers tools for "how to calm down a panicking person," including breathing techniques.[195]

Despite these measures to protect and defend against hybrid threats, Romania faces several challenges in preparing its population for disruptions to goods and services caused by manmade or natural disasters to its CI.

First, as revealed in the 2024 elections, Romania struggles with malign influence, especially through social media, and the ability to send credible information to its population. A 2022 report on disinformation in Romania argues that, similar to other countries, Romania faces a disinformation crisis fueled by malign social media personas, which are believed to have ties to the Kremlin. "These meticulously curated topics include the low level of trust in state institutions and politicians, apprehension that the country risks losing its cultural identity in a globalizing world, nationalism and perceptions that the EU imposes overbearing regulations."[196] Campaigns like these undermine trust in the government, which, in the event of disruptions to goods and services, could hinder the government's ability to message its population effectively and control panic.

Second, and connected to disinformation campaigns, Romania struggles with the rise of far-right politics, which aim to disrupt its democracy and government. The Alianţa pentru Unirea Românilor (The Alliance for the Unification of Romanians, AUR), which was founded in 2019, campaigns on an anti-EU, anti-NATO, and pro-Russian platform, capitalizes on narratives of culture and family values, and is believed to be influenced by the Kremlin.[197] Georgescu, who won the most votes in Romania's presidential elections in 2024, ran on a similar platform, but as an independent. Elena Calistru and Laura Burtan argue that these far-right politicians aim to undermine the credibility of the democratic system and the Romanian government with tacit or explicit support from the Kremlin. In a crisis, this lack of confidence and legitimacy in the government will most likely affect its ability to communicate with and defend its population.[198]

192 "Guide for Crisis Situations," 21.
193 "Guide for Crisis Situations," 24.
194 "Guide for Crisis Situations," 11.
195 "Guide for Crisis Situations," 9.
196 Elena Calistru and Laura Burtan, "Anti-Western Narratives in Romania," *Funky Citizens*, 2022, accessed June 14, 2025, https://www.globsec.org/sites/default/files/2022-02/Anti-Western-Narratives-in-Romania.pdf, 2.
197 Calistru and Burtan, "Anti-Western Narratives in Romania."
198 Calistru and Burtan, "Anti-Western Narratives in Romania."

Key Takeaways from Case Studies

Europe's experiences with preparing populations for disruptions to goods and services caused by both natural and manmade disasters to CI provide useful insights for how to build societal resilience as a form of national defense against hybrid threats.

These case studies provide the following takeaways:

- NATO and the EU provide overarching guidelines and requirements for defending CI and for providing continuity of critical goods and services in times of crisis, which should create a baseline across member countries and mitigate the effects of cascading disruptions across borders.
- Sweden, the UK, and Romania each have different definitions of CI. All three countries identify the four "lifeline" sectors of energy, water, communications, and transportation infrastructure, but each country includes additional sectors as well. Sweden does not define specific CI sectors but rather how CI supports vital societal functions (VSF), which should help the government to understand the goods and services each sector provides and how disruptions might affect the population. This knowledge, in turn, should help a country prepare for the possibility of these disruptions, including building societal resilience against these disruptions, irrespective of the cause.
- Sweden, the UK, and Romania have all experienced hybrid threats against their CI, including cyberattacks, but also physical sabotage. Russia is the principal threat actor and is supported by individuals and organizations acting on behalf of or sympathetic to Russia. All three countries have stressed that these attacks are impossible to prevent and therefore require preparing the population for disruptions to life-giving goods and services.
- Sweden, the UK, and Romania each have national strategies and policies designed to address cyberattacks against CI. These strategies are relatively new and being updated as threats develop and administrations change. All three countries have experienced the threat or actual incidents of physical sabotage against CI.
- Romania and the UK have organizations outside the government designed to prepare populations for disruptions of goods and services. These organizations are apolitical and should provide continuity of information and messaging across changes in administrations and in areas of political and ethnic division.
- Sweden and Romania have guidebooks designed to prepare populations for crises, including goods to have on hand, instructions for what to do in a crisis, and a basic communications strategy. Both guidebooks are available in several languages and stress a communal approach to preparing for and defending against crises. Sweden mails a paper copy to each household to have on hand in the event of electrical and mobile phone disruptions.

4. Best Practices for Preparing Populations for Hybrid Attacks

Hybrid threats are not going away any time soon. In fact, it is likely that adversaries will continue to use hybrid threats with increasing frequency because they are a means of offsetting the United States, NATO, and other countries' conventional military capabilities without direct confrontation and attribution.

Russia has used a range of hybrid threats in Europe to attack CI, including sabotage on cables and pipelines in the Baltic Sea, cyberattacks against Britain's National Health System and other sites in the UK, and both cyberattacks and a foiled physical attack on CI in Romania. Hybrid attacks like these have caused disruptions of goods and services and have undermined trust in governments' ability to defend their CI and the population.

The International Institute for Strategic Studies in the UK issued a report in August 2025 that enumerates Russian attacks on CI in Europe since 2022, and notes that in 2024, confirmed Russian attacks on European CI had gone up 246 percent from the previous year alone.[199] The report stresses that Russia's hybrid attacks on European CI is part of a wider strategy of *gibridnaya voyna*, or "coercive actions with an emphasis on using all tools of the state and associated non-state actors to achieve political power," and to destabilize and weaken Europe.[200]

Also in August 2025, Norway revealed that one of their hydroelectric dams had suffered a cyberattack in April that caused 500 liters of water per second to flow from the dam for four hours before it was detected and stopped. Norway's head of Police Security Service, Beate Gangaas, unequivocally blamed Russia for the attack. She argued that "the aim of this type of operation is to influence and to cause fear and chaos among the general population." She further implored, "I want Norwegians to be prepared."[201]

These state-driven attacks are not going to stop, and it is unlikely that they can be completely prevented. Therefore, preparing populations for the physical and psychological effects of these activities is urgently needed.

The case studies of Sweden, the UK, and Romania provide **seven key takeaways** for preparing populations for disruptions to goods and services caused by hybrid threats and other hazards.

1. Define CI by its relationship to the population

There is no universal agreed-to definition of CI. Most countries' definitions include the four "lifeline" sectors of energy, water, transportation, and communications, with subsectors depending on a country's geography and size.

Rather than name specific CI sectors, Sweden's action plan focuses on a functional definition of CI and the services it provides the population, arguing that CI is anything which "a loss of or a severe disrup-

199 Edwards and Seidenstein, "The Scale of Russian Sabotage Operations Against European Critical Infrastructure," 9.
200 Edwards and Seidenstein, "The Scale of Russian Sabotage Operations Against European Critical Infrastructure," 9.
201 Nerijus Adomaitis, "Norway Spy Chief Blames Russian Hackers for Dam Sabotage in April, *Reuters*, August 13, 2025, https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/.

tion to the activity that alone or together with other similar events, rapidly leads to a serious societal emergency or crisis." It calls this dynamic between CI and the population vital societal functions (VSF).

Furthermore, this definition allows for flexibility in which CI sectors should be considered vital to the population in response to specific threats and moves beyond the four lifeline sectors of energy, water, communications, and transportation infrastructure. The financial sector, for example, should be included based on the critical role it plays in the daily life and security of the population.

Sweden's approach to identifying CI and the VSF it performs should help a country understand the goods and services each sector provides and how disruptions might affect the population. This knowledge, in turn, should help a country prepare for the possibility of these disruptions, including building societal resilience against these disruptions, irrespective of the cause.

2. Harden CI with good cyber strategies and defense against physical sabotage

Sweden, the UK, and Romania have all experienced a range of hybrid attacks against their CI. Cyberattacks, including DDoS, malware, ransomware attacks, and cyber espionage, are arguably the biggest threat to CI. Each of these countries has developed cyber strategies, policies, and agencies for addressing cybersecurity.

In addition to creating cyber strategies, policies, and its NCSC, the UK government has also set up a public-private collaborative, Cyber-Security Information Sharing Partnership (CISP), as a platform for cybersecurity professionals to collaborate with each other and with the government on cyberthreats and by creating what it calls "trust groups." Public-private partnerships like CISP should help mitigate the gaps and seams in CI protection against cyberattacks and potentially other threats as well.

Additionally, physical sabotage to CI should not be overlooked as a potential hybrid attack. Europe has experienced a wave of physical attacks on CI, including the Nord Stream 2 attack in 2022 and a series of attacks against underseas cables beginning in 2023. Sweden and Romania have both reported physical sabotage to their CI since Russia's full-scale invasion of Ukraine in 2022, and the UK has named sabotage as a potential threat that could "turn off the lights" for its people. This is a trend that is likely to continue and could make energy and communications cables vulnerable to physical attack.

Defending against physical sabotage requires physically hardening CI and improving intelligence aimed at identifying saboteurs and types of attacks on CI.

3. Create policies and guidelines that establish a baseline of preparedness

Crises, including hybrid threats, rarely stop at a country's borders. A crisis in one country will most likely affect neighboring countries, regions, and possibly the world. Russia's hybrid warfare against Ukraine and its allies, the mass migration crisis of 2015, the Covid-19 pandemic of 2020–2022, and the 2025 power outage on the Iberian Peninsula are all examples of crises that crossed borders and affected regions.

In response to these crises, the EU created guidelines and policies to establish a baseline of preparedness across member countries, including against hybrid threats. The EU stood up a hybrid threat task force;

established the "Joint Framework on Countering Hybrid Threats," as well as the "Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats;" introduced annual reports chronicling hybrid threats and progress in countering these activities; and adopted "The European Council Conclusions," which includes "the possibility for the Member States to invoke the Solidarity Clause (Article 222 TFEU) in addressing a severe crisis resulting from hybrid activity.[202]

NATO also has taken steps designed to build resilience. It drafted the Seven Baseline Requirements for National Resilience in 2016 with the goal of addressing regional crises from a broad security perspective, including hybrid threats. The seven requirements focus on policies and physical preparedness for key national resources, including continuity of government, medical care, transportation, and information. A 2022 report proposed additional pillars of payment systems, psychological resilience, and data protection as necessary for enhancing preparedness and societal resilience.[203] And in 2023, a joint EU-NATO Task Force on Resilience of Critical Infrastructure was created to address gaps between the military, intelligence community, and law enforcement.[204]

Additionally, Nordic countries are currently creating their own regional strategy and guidelines for disaster preparedness, what it calls an "all hazards approach," that includes addressing supply chain vulnerabilities and creating reserve funds for crises.

Overarching efforts to create similar levels of preparedness across countries, regions, and alliances should, in theory, help mitigate disruptions of goods and services for a range of threats, both manmade and natural, and reduce possible "spillover" effects from one country or region to the next.

4. Publicly call out states using hybrid threats

Russia has capitalized on proxies and other third-party actors to carry out a range of hybrid attacks, in addition to exploiting gaps and loopholes in international law, what is often called "lawfare," to perpetrate hybrid attacks against its adversaries.

Sweden, Romania, and the UK have all deliberately called out Russia as the state actor responsible for hybrid attacks against their countries, despite the fact that most of these attacks cannot be legally proven to have come from the Kremlin.

Nevertheless, these countries are making a political stand by calling out hostile acts inside their countries and informing their populations of Russia's malign intentions. The UK's NCSC's 2023 annual report, for example, unequivocally states: "These state-aligned actors might seemingly offer the Russian state 'plausible deniability' in its attacks, but that is where attributions by the UK government and our allies, together with technical advisories by the NCSC are critical in unmasking the Russian state's intent and holding such actors to account."[205]

Calling out Russia as the perpetrator behind cyberattacks and sabotage to CI is important for building consensus on the need for a political, economic, and possible military response to these acts and deny-

202 "Hybrid Threats," European Commission, accessed May 4, 2025, https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en.
203 Christie and Berzina, "NATO and Societal Resilience: All Hands on Deck in an Age of War."
204 Edwards and Seidenstein, "The Scale of Russian Sabotage Operations Against European Critical Infrastructure," 12.
205 "Annual Review 2023," 19.

ing Russia and other state actors persistent deniability of their aggression. It is also an important step in explaining hybrid threats, preparing populations for these attacks, and demonstrating that governments are aware of the threat and fighting it.

5. Physically and psychologically prepare populations before a CI crisis

In addition to physically hardening CI and improving cybersecurity, NATO, the EU, and the countries studied have called for building societal resilience as a means of defending and potentially deterring hybrid attacks that target populations.

Building societal resilience includes both physical and psychological preparation of the population.

Physical preparations should include the necessary goods to have for a specified period of time. In 2025, the EU called for all citizens to be able to sustain a crisis for seventy-two hours without government help, and included keeping food, water, medicine, a radio, a battery charger, and cash on hand. Sweden and Romania also have included instructions on what to have on hand, in what amounts, and the period of time these goods should last. Additionally, physical preparations for a crisis should include where to go in the event of specific crises, including evacuation plans; a communications strategy, including how to get messages to and from one another and from the government in the event of cell phone, internet, and/or electrical disruptions; and what to do in the event of specific crises, including both natural and manmade disasters.

Psychologically preparing the population is equally important for disaster preparedness and should help to minimize panic and bolster societal resilience. Populations should be educated about the nature of hybrid threats and the critical role they play in undermining these attacks by not "taking the bait" and panicking, turning on each other, or losing trust in the government. When done properly, psychological preparations should be empowering to the population, not frightening.

Put together, physically and psychologically preparing populations for the possibility of disruptions caused by hybrid attacks should reinforce one another and work to build societal resilience.

Sweden and Romania have created guidebooks designed to prepare their populations for a spectrum of crises, ranging from dis- and mal-information to natural disasters to war and occupation. These guidebooks are short, issued in several languages, and include illustrations and simple-to-follow instructions, making them useful to the widest number of people.

Critically, Sweden has mailed physical copies to all households to have on hand. This step is important in the event of loss of electricity, Wi-Fi, and/or cellphone reception, which would prevent individuals from accessing this information online in a crisis.

6. Inform populations of their role in mitigating hybrid threats

Hybrid threats that target populations aim to cause panic, which in turn magnifies the effects of an attack and undermines confidence in a government's ability to protect its citizens. Explaining the strategy of hybrid threats and preparing populations for disruptions should help undermine the adversary's plan.

One approach for explaining the strategy of hybrid threats is to compare it to terrorism. Hybrid threats are deliberate, malicious acts that can occur anywhere and at any time and are executed with the aim of causing fear and panic in the population.

However, hybrid threats and terrorism have at least one important distinction. Terrorists usually claim recognition for their actions as a form of publicity whereas perpetrators of hybrid threats aim to carry out attacks without direct attribution, and often without detection. This approach makes clearly attributing hybrid attacks to the perpetrator difficult and should also be included in explaining the nature of hybrid threats as a means of preparing populations.

Informing populations that they have a role to play in mitigating the effects of hybrid attacks is important. If done properly, this should be empowering to the population, not frightening. Sweden, for example, emphasizes that, "To resist these threats, we must stand united. If Sweden is attacked, everyone must do their part to defend Sweden's independence—and our democracy. We build resilience every day, together with our loved ones, colleagues, friends, and neighbours."[206]

Romania emphasizes a similar approach in its crisis guidebook: "Help people around you under the direction of authorities, donate blood, volunteer, offer help or information when requested by authorities, and obey applicable laws on your own initiative! The greater the solidarity between citizens, the easier and faster we will overcome any crisis." [207]

7. Non-governmental organizations may be useful for consistent messaging

The UK and Romania have created independent, apolitical organizations dedicated to disaster preparedness and building societal resilience. These organizations may be helpful in providing continuity of information and messaging across administrations and in politically, ethnically, and socially divided countries.

In 2020, the UK founded the NPC during the Covid-19 crisis to "promote policies and actions to help the UK be significantly better prepared to avoid, mitigate, respond to, and recover from major shocks, threats and challenges."[208] Broadly speaking, its mandate is to build societal resilience, including against disruption of goods and services cause by hybrid threats. In 2024, the UK held parliamentary elections in which the Labor Party received the majority of votes, ending fourteen years of Conservative Party rule. In theory, the NPC should continue its work irrespective of this major shift in government and changes in policy.

Romania stood up the E-ARC in 2022 as a "centre of excellence in the field of resilience" as "a partner of NATO and the EU, acting for the benefit of these organisations, as well as Member States or partners."[209] As with the NPC, E-ARC should provide continuity in best practices for building resilience irrespective of Romania's government, and developments within NATO and the EU.

206 *In Case of Crisis or War,* 3.
207 "Romanian Guide for Crisis Situations," 11.
208 "About," UK National Preparedness Commission.
209 "Euro-Atlantic Resilience Centre Mission Statement."

Challenges

In addition to best practices, this research revealed three challenges to preparing populations for disruptions to goods and services caused by hybrid threats to CI.

1. **Finding the right balance in explaining the threat to populations is difficult**

   Governments and organizations need to find the right balance between threat, urgency, and empowerment when messaging the population about hybrid threats.

   On the one hand, if the threat is presented as too prevalent and too dire, the message itself could cause populations to panic or react in a way that is negative to the normal functioning of society. In other words, the message could be more damaging than the threat, as some argue the "duck and cover" messaging was to U.S. children during the Cold War. On the other hand, underselling the threat could cause people to not take the message seriously and not prepare.

   Similarly, "crying wolf"—falsely predicting that a threat is imminent—might cause people to not take future messaging seriously, which could also result in populations not being prepared for crises. Finding the right balance of when to "sound the alarm bells" of an imminent threat is also important and difficult to do.

   Finding the right balance in messaging, therefore, is crucial and will most likely require country-specific, regional-specific, and even population-specific messaging.

2. **Effectively messaging divided populations requires a trusted messenger**

   All the countries studied have either politically or ethnically divided societies, or both.

   Sweden is currently grappling with messaging and preparing its ethnically diverse population as part of Total Defence, which relies on a community approach and national unity for defending the country and its people. What it means to be Swedish appears to be in flux, which in turn may affect its Total Defence messaging and preparation.

   A politically divided country also faces challenges with preparing its population for disruptions of goods and services caused by hybrid threats. If a country's administration is only trusted by the population that voted for it, the rest of the population may not heed its messages to prepare.

   To address political and ethnic divisions, Romania and the UK have both created apolitical organizations aimed at bridging these gaps, E-ARC and the NPC, respectively. These organizations are only a few years old and their effectiveness in messaging and preparing populations for disaster and resilience remains to be seen.

   Overall, preparing populations for disruptions of goods and services caused by hybrid threats requires a trusted messenger. If the government is not trusted by a portion of the population, additional messengers may be required.

3. Creating measures of effectiveness (MOE) for preparedness is difficult

The most accurate way to measure a population's disaster preparedness is to observe how the population responds in an actual crisis. However, if the population is unprepared, it is too late to correct these deficiencies, and the government is left with a crisis. Moreover, some grave challenges may never come to pass but still require the population to be prepared given the severity of the threat, such as nuclear war. Therefore, governments need MOEs for disaster preparedness programs prior to a crisis.

MOEs for preparing populations to resist, withstand, and recover from disruptions to goods and services caused by hybrid threats should include both physical preparedness and psychological preparedness.

Arguably, **physical preparedness** is easier to measure because it can include specified amounts per household of provisions, like food, water, medicine, fuel, and so on. Governments can instruct households how much to have on hand and then measure the effects of this messaging through surveys or other means. FEMA, for example, conducts an annual survey to assess household preparedness for natural disasters in the United States, as described in Chapter 2.

MOEs for **psychological preparedness** are more difficult. Several scholars have offered models for measuring a population's "will to fight," which includes psychological preparedness. Robert Burrell, for example, proposes a model for measuring state resilience, including societal resilience, as a necessary capability for a population to fight and resist a military invasion. He proposes, "some key factors to consider when measuring resiliency include: (a) the physical aspects of the nation or region in question, (b) the fragility of current governance, (c) cultural resilience to change, (d) the will of the population to fight, and (e) the perceived effectiveness of current governance." He includes using databases such as the human fragility index, SwissRE, the Central Intelligence Agency (CIA) World Fact Book, and the World Bank as potential metrics of resilience, arguing a correlation between geography, levels of governance, economic health, and societal resilience and resistance to invasion and war.[210]

Somewhat similarly, Ben Connable outlines two models for measuring a country's will to fight, focusing on "holism," or looking at culture as a complex system, and rejecting "reductionism," or reducing a nation's culture into a few key variables. Connable notes that holism takes longer and requires more granular information on a country that may or may not be available but ultimately produces a better predictor for a nation's will to fight.[211]

Both Burrell and Connable are concerned primarily with measuring a population's will to fight in the extremity of war and its ability to withstand physical invasion. While these approaches may be useful for understanding resistance under these circumstances, measuring societal resilience in the face of less extreme and overt but still threatening incidents, like disruptions to goods and services caused by hybrid threats, may require different metrics and methods of measurement.

As part of its Total Defence, Sweden measures the population's "will to defend," as opposed to will to fight, as a specific subset of societal resilience. Its government defines the will to defend as "(*a*) a char-

210 Robert S. Burrell, "A Guide for Measuring Resiliency," Irregular Warfare Initiative, January 16, 2024. https://irregularwarfare.org/articles/a-guide-for-measuring-resiliency/#:~:text=Some%20key%20factors%20to%20consider,perceived%20effectiveness%20of%20current%20governance.

211 Ben Connable, "Structuring Cultural Analyses Applying the Holistic Will-to-Fight Models," *Journal of Advanced Military Studies* (2022).

acteristic of the individual; and (*b*) represents a mental state of support for the total defence of the country." Furthermore, Tarja Cronberg argues that the will to defend is "an individual's state of mind during peacetime, as opposed to the will to fight, which: (*a*) is a phenomenon related to a group, community or society; and (*b*) represents an attitude of or capacity for standing against threats of violence."[212]

Sweden, therefore, measures the will to defend as: a mental state during peacetime; measured at the individual level; how the individual relates to the group (society, community); and as an "attitude of or capacity for standing against threats of violence."

Sweden's principal method of measuring the will to defend is through household surveys, which includes asking if individuals are "willing to defend their country by weapons in all situations, even when the outcome is uncertain."[213] Cronberg notes that Sweden uses other metrics, including conscription rates and attitudes toward territorial defense.[214] Cronberg's analysis was written in 2005, during the "peace dividend" years following the collapse of the Soviet Union. Sweden and other Nordic countries have undoubtedly updated surveys and other metrics following Russia's illegal annexation of and full-scale war on Ukraine in 2014 and 2022, respectively.

Creating the right MOEs for assessing populations' physical and psychological preparedness for disruptions of goods and services caused by hybrid threats remains a challenge that requires more study.

212 Tarja Cronberg, "The Will to Defend: A Nordic Divide Over Security and Defence Policy," in *The Nordic Countries and the European Security and Defence Policy,* eds. Alyson J. K. Bailes, Gunilla Herolf, and Bengt Sundelius (Oxford University Press, 2006).

213 Cronberg, "The Will to Defend: A Nordic Divide Over Security and Defence Policy," 316.

214 Cronberg, "The Will to Defend: A Nordic Divide Over Security and Defence Policy."

Select Bibliography

Adamson, Eric and Jason Moyer. "In From the Cold: Rebuilding Sweden's Civil Defense for the NATO Era." *War on the Rocks.* April 9, 2024. https://warontherocks.com/2024/04/in-from-the-cold-rebuilding-swedens-civil-defense-for-the-nato-era/.

Bertilsson, Fredrik. "The Swedish Defence Research Establishment (FOA) and the Influence of Historical Knowledge on Swedish Civil Resistance Policy." *Scandinavian Journal of History* 46, no. 4 (2021).

Burrell, Robert S. "A Guide for Measuring Resiliency," Irregular Warfare Initiative, January 16, 2024. https://irregularwarfare.org/articles/a-guide-for-measuring-resiliency/#:~:text=Some%20key%20factors%20to%20consider,perceived%20effectiveness%20of%20current%20governance.

Calistru, Elena and Laura Burtan. "Anti-Western Narratives in Romania." *Funky Citizens*. 2022. https://www.globsec.org/sites/default/files/2022-02/Anti-Western-Narratives-in-Romania.pdf.

Christie, Edward Hunter and Kristine Berzina. "NATO and Societal Resilience: All Hands on Deck in an Age of War." *The German Marshall Fund of the United States Policy Brief.* July 2022. https://www.gmfus.org/sites/default/files/2022-07/NATO%20and%20Societal%20Resilience%20All%20Hands%20on%20Deck%20in%20an%20Age%20of%20War.pdf.

"Combating Terrorism: FEMA Continues to Make Progress in Coordinating Preparedness and Response." Government Accountability Office. March 20, 2001. Accessed June 20, 2025. https://www.gao.gov/products/gao-01-15.

Connable, Ben. "Structuring Cultural Analyses Applying the Holistic Will-to-Fight Models," *Journal of Advanced Military Studies* (2022).

"Critical Infrastructure Resilience at EU-Level," European Commission, September 23 2024. Accessed May 10, 2025. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en.

Cronberg, Tarja. "The Will to Defend: A Nordic Divide Over Security and Defence Policy." In *The Nordic Countries and the European Security and Defence Policy.* Eds. Alyson J. K. Bailes, Gunilla Herolf, and Bengt Sundelius. Oxford University Press, 2006.

"Countering Hybrid Threats." North Atlantic Treaty Organization. Accessed December 6, 2024. https://www.nato.int/cps/en/natohq/topics_156338.htm.

Crowther, G. Alexander. "NATO and Hybrid Warfare: Seeking a Concept to Describe the Challenge from Russia." In *Hybrid Warfare: Security and Asymmetric Conflicts in International Relations.* Eds. in Mikael Weissmann, et al. I.B. Tarus, 2021.

De Coning, Cedric. "Hybrid COE Working Paper No. 9: Strengthening the Resilience and Adaptive Capacity of Societies at Risk from Hybrid Threats." Hybrid COE. June 2021. https://www.hybridcoe.fi/publications/

hybrid-coe-working-paper-9-strengthening-the-resilience-and-adaptive-capacity-of-societies-at-risk-from-hybrid-threats.
Edwards, Charlie and Nate Seidenstein. "The Scale of Russian Sabotage Operations Against European Critical Infrastructure." International Institute for Strategic Studies. August 2025. https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure/.

"Emergency Management: FEMA Has Made Progress, but Challenges and Future Risks Highlight Imperative for Further Improvements." Government Accountability Office. June 25, 2019. https://www.gao.gov/products/gao-19-617t.

Evans, Carol V., ed. *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency*. U.S. Army War College Press, 2022.

Galeotti, Mark. *The Weaponization of Everything: A Field Guide to the New Way of War.* Yale University Press, 2022.

Gregg, Heather S. "The Human Domain and Influence Operations in the 21st Century." *Special Operations Journal* 2, no. 2. (2016).

-----. "Hybrid Threats and Strategic Competition," *Connections QJ* 23, no. 2 (2024).

"Guide for Crisis Situations." Government of Romania. 2024. https://e-arc.ro/wp-content/uploads/2024/06/Guide-EN.pdf.

Häkkinen, Teemu and Miina Kaarkoski. "Willingness to Defend and Foreign Policy in Sweden and Finland from the Early Cold War Period to the 2010s." *Scandinavian Journal of History* 49, No. 2 (2024).

Hastings, Rob. "How the UK's Emergency Electricity Rationing Plans Could Work This Winter." *The iPaper.* October 8, 2022. https://inews.co.uk/news/uk-blackout-plans-government-emergency-strategy-winter-electricity-rationing-1899998?ico=in-line_link.

----- "The Disaster Awaiting Us if a Cyber Attack Cuts All the UK's Electricity." *The iPaper.* December 25, 2023. https://inews.co.uk/news/technology/ministers-fear-cyber-attack-cutting-electricity-2809348.

"Hurricane Katrina: 10 Years After the Storm." Government Accountability Office. August 27, 2015. https://www.gao.gov/blog/2015/08/27/hurricane-katrina-10-years-after-the-storm.

"Hurricane Katrina: Better Plans and Exercises Need to Guide the Military's Response to Catastrophic Natural Disasters." Government Accountability Office. May 26, 2006. https://www.gao.gov/products/gao-06-808t.

"In Case of Crisis or War." The Swedish Civil Contingencies Agency (MSB). 2024. https://rib.msb.se/filer/pdf/30874.pdf.

Jenkins, Brian Michael and Bruce R. Butterworth. "Does "See Something, Say Something" Work?" Mineta Transportation Institute. SP11-18. December 2018. https://transweb.sjsu.edu/research/SP1118-See-Something-Say-Something.

"Joint Statement of the NATO-Ukraine Commission." North Atlantic Treaty Organization. September 4, 2014. https://www.gov.uk/government/publications/nato-summit-2014-joint-statement-of-the-nato-ukraine-commission/joint-statement-of-the-nato-ukraine-commission.

Kalniete, Sandra and Tomass Pildegovičs. “Strengthening the EU’s Resilience to Hybrid Threats.” *European View* 20, No. 1 (2021).

Kilcullen, David. *The Dragons and the Snakes: How the Rest Learned to Fight the West* Oxford University Press, 2020.

Lallerstedt, Karl. “Rebuilding Total Defense in a Globalized Deregulated Economy: The Case of Sweden.” *Prism* 9, no. 23 (2021).

Malmberg, Pär, Jan Ottosson, Martin Eriksson, Olle Jansson. “The Role of Industry Sweden’s Total Defence: Past, Present, and Future.” The Royal Swedish Academy of War Sciences. September 26, 2023. https://kkrva.se/the-role-of-industry-in-swedens-total-defence-past-present-and-future/.

Milmo, Dan. “Russia Can Turn the Lights Off: How the UK is preparing for Cyberwar.” *The Guardian*. December 3, 2024. https://www.theguardian.com/technology/2024/dec/03/russia-can-turn-the-lights-off-how-the-uk-is-preparing-for-cyberwar.

“NATO’s Military Concept for Defence Against Terrorism.” North Atlantic Treaty Organization. August 19, 2016. Accessed March 22, 2025. https://www.nato.int/cps/en/natohq/topics_69482.htm#:~:text=The%20unlawful%20use%20or%20threatened,political%2C%20religious%20or%20ideological%20objectives.

“Resilience, Civil Preparedness and Article 3.” North Atlantic Treaty Organization. November 13, 2024. Accessed March 23, 2025. https://www.nato.int/cps/bu/natohq/topics_132722.htm.

Roepke, Wolf-Diether and Hasit Thankey. “Resilience: The First Line of Defence.” *NATO Review.* February 27, 2019. https://www.nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html.

Rohart, Marius Laurentiu. “Overview of Critical Infrastructure Protection in Romania.” The 9th International Scientific Conference, “Defense Resource Management in the 21st Century.” Braşov, Romania. November 14, 2014. https://codrm.eu/wp-content/uploads/2024/12/32_Rohart.pdf.

“Terrorism Preparedness.” The American Red Cross. Accessed June 20, 2025. https://www.redcross.org/get-help/how-to-prepare-for-emergencies/types-of-emergencies/terrorism.html.

“Total Defence.” Government Offices of Sweden. Accessed March 26, 2025. https://www.government.se/government-policy/total-defence/.

“The UK Government Resilience Framework.” Government of the UK. Accessed June 4, 2025. https://www.gov.uk/government/publications/the-uk-government-resilience-framework/the-uk-government-resilience-framework-html.

“Annual Review 2023.” UK National Cyber Security Centre. 2023. https://www.ncsc.gov.uk/collection/annual-review-2023.

“The Gray Zone.” U.S. Special Operations Command. 2015. https://info.publicintelligence.net/USSOCOM-GrayZones.pdf.

“Wales Summit Declaration.” North Atlantic Treaty Organization. September 2014. https://web.archive.org/web/20150621015842/https://www.gov.uk/government/uploads/system/uploads/attachment_data/

file/351406/Wales_Summit_Declaration.pdf.
Weissmann, Mikael, Niklas Nilssen, Björn Palmertz, Per Thunholm (eds.). *Hybrid Warfare: Security and Asymmetric Conflicts in International Relations.* I.B. Tarus, 2021.

Wigell, Mikael, Mariette Hägglund, Christian Fjäder, Emma Hakala, Johanna Ketola, and Harri Mikkola. "Nordic Resilience: Strengthening Cooperation on Security of Supply and Crisis Preparedness." *FIIA Report*, No. 70. September 2022. https://fiia.fi/en/publication/nordic-resilience.

Select Websites

Center for Strategic & International Studies Gray Zone Project. Accessed March 21, 2025. https://www.csis.org/programs/gray-zone-project.

"Euro-Atlantic Resilience Centre." Accessed February 3, 2025. https://e-arc.ro/en/2024/03/18/e-arc-mission-statement/.

"How FEMA Works." Federal Emergency Management Agency. Accessed April 10, 2025. https://www.fema.gov/about/how-fema-works.

Hybrid European Center of Excellence. August 13, 2025. https://www.hybridcoe.fi/.

"Hybrid Threats." European Commission. Accessed May 4, 2025. https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en.

The National Cyber Security Centre. Accessed June 4, 2025. https://www.ncsc.gov.uk/.

"National Household Survey." Federal Emergency Management Agency. Accessed April 17, 2025. https://www.fema.gov/about/openfema/data-sets/national-household-survey.

"Coordinating Centre for Protection of Critical Infrastructure." Ministry of Internal Affairs of the Government of Romania. Accessed June 12, 2025. https://www.mai.gov.ro/en/coordinating-centre-for-protection-of-critical-infrastructure/.

Swedish Psychological Defence Agency. Accessed July 7, 2025. https://mpf.se/psychological-defence-agency/about-us/our-mission.

UK National Preparedness Commission. Accessed June 6, 2025. https://nationalpreparednesscommission.uk/about/.

"War in Our Time." Försvarsmakten (YouTube). Accessed June 1, 2025. https://www.youtube.com/playlist?list=PLGXVHglmhBQI4-E55p7q8ngE_-L-GuK3g.