Civic Cyber Defence/Resilience: A Review of Approaches

Matthew Warren[1], Marius Laurinaitis[2] and Inga Malinauskaitė-van de Castel[2]
[1]RMIT University, Melbourne, Australia and University of Johannesburg, South Africa
[2]Mykolas Romeris University, Vilnius, Lithuania

Matthew.warren2@rmit.edu.au
laurinaitis@mruni.eu
inga.malinauskaite@mruni.eu

Abstract: Cyber defence / security is a critical component of civic resilience, ensuring the protection and continuity of essential services and infrastructure in the face of cyber threats. As societies become increasingly digital, the potential for cyber attacks on public systems, such as utilities, healthcare, transportation, and government services, grows. These attacks can disrupt daily life, compromise sensitive data, and undermine public trust. But what happens in a national emergency? How is cyber security and disinformation considered from a civic cyber resilience perspective? What are the expectations of citizens in the first 72 hours of a national emergency? The paper will evaluate cyber advice offered to the citizens of a number of European countries. The evaluation will focus on the national advice offered from a technological, legal, and societal perspective. The analysis will focus on the different approaches of six European countries and what can be learned from these different approaches regarding Civic Defence and Resilience.

Keywords: Cyber defence and resilience, Cyber security, Disinformation and society

1. Introduction

Cyber security is a critical component of civic resilience, ensuring the protection and continuity of essential services and infrastructure in the face of cyber threats. As societies become increasingly digital, the potential for cyber attacks on public systems, such as utilities, healthcare, transportation, and government services, grows. These attacks can disrupt daily life, compromise sensitive data, and undermine public trust.

Moreover, cyber security fosters public confidence in digital services, encouraging the adoption of new technologies that can improve efficiency and quality of life. It also supports economic stability by protecting businesses and financial institutions from cybercrime, which can have far-reaching consequences for local economies.

Effective cyber security measures help safeguard national systems against unauthorised access, data breaches, and other malicious activities. By implementing robust cyber security protocols, countries can enhance their ability to prevent, detect, and respond to cyber incidents. This proactive approach not only mitigates the immediate impact of cyber attacks but also contributes to long-term resilience by maintaining the functionality and reliability of critical services strengthening civic resilience. Disinformation is false or misleading content that is spread with the intention to deceive or secure economic or political gain, and which may cause public harm. Misinformation is false or misleading content shared without harmful intent, though the effects can still be harmful (European Union, 2024). The spread of both disinformation can have a range of harmful consequences, such as threatening our democracies, polarising debates, and putting the health, security and environment of EU citizens at risk. Steps in helping societies identify and dismiss disinformation will be a major step in reducing the impact of disinformation.

The concept of Cyber Civic Resilience (CCR) refers to the capacity of citizens to use cyber services securely during times of insecurity and in ways that strengthen overall resilience (Wepner & Wester, 2015). In terms of this CCR concept - 'Cyber' involves computers and networks, 'civic' relates to a citizen's perspective, and 'resilience' is the ability to maintain or improve functionality after disruption. CCR is important because society increasingly relies on online services, making citizens vulnerable if these services fail. Furthermore, citizens are recognised as a major source of disinformation e.g. citizens spreading disinformation and rumours and also citizens being targets of cyber security attacks. Understanding and strengthening CCR is crucial for societal security in the digital age, considering the issues of cyber defence and disinformation.

This paper will explore what happens in a national emergency in terms of how cyber defence (referred to in this paper as cyber security) and disinformation are considered from a civic resilience perspective. The paper will evaluate advice offered to the citizens of countries within Europe and what can be learned from these different approaches in relation to cyber security and disinformation.

2. Country Examples

In terms of the paper, we will look at the approaches taken by a number of European countries in regard to offering advice to citizens. The country examples are grouped as follows:

Baltic Countries

Estonia

The Estonian government's official crisis preparedness website provides essential information on how to prepare for and respond to emergencies. The site covers topics such as (Estonian Government, ND):

- Crisis Preparedness – Guidance on making an emergency plan, assembling a crisis supply kit, and understanding risks like natural disasters, cyber threats, and military conflicts;
- Emergency Response – Steps to take during different crises, including power outages, cyber attacks, and extreme weather;
- Government Alerts & Actions – Updates on national security, civil protection measures, and official recommendations;
- Support & Resources – Contacts for emergency services, psychological support, and ways to help others in a crisis.

The Estonian government (Estonian Government, 2022a) offers advice to citizens and businesses about cyber security and disinformation, in terms of:

- Being suspicious of sources of information, e.g. suspicious e-mails that you have received;
- Citizens should have proper cyber hygiene in place, e.g. updating software, using antivirus software, using strong passwords, using multi-factor authentication, and backing up key information;
- Citizens to consider their digital footprint and not publicise their personal information;
- Businesses should have incident management plans in place, adhere to certain security levels, implement incident management plans and have in place past incident analysis strategies.

There are also individual guides that citizens can download for their reference such as *What to do in a crisis situation? Be prepared!* (Estonian Government, 2022b). This guide covers a whole range of information about preparing for emergencies including cyber security, but also disinformation and information warfare, in terms of citizens applying critical thinking to what they read online, not sharing false information, reporting any false information that citizens see online and then block those sources and only trust information from official sources such as the national broadcaster.

The Estonian government widely shares its citizen focused information, including a number of sources such as web pages, PDF documents that can be downloaded and social media channels (see Figure 1).

Figure 1: Estonian Government Instagram Feed: Reminding citizens to check that mobile battery rechargers are charged for an emergency

Latvia

The Latvian government (Ministry of Defence) has developed a citizen advice guide - *What to Do in Case of Crisis*. The guide is aimed at the first 72 hours of a crisis to help Latvian citizens prepare for and respond to emergencies, including military conflicts and natural disasters.

Key areas that the guide covers include (Latvian Government, 2025):

- Crisis Preparedness – How to prepare an emergency plan, assemble a survival kit, and stay informed through official channels;
- Immediate Actions – Steps to take if a crisis occurs, such as seeking shelter, securing food and water, and following government instructions;
- Military Threats & Occupation – Guidance on what to do in case of an invasion, how to recognise disinformation and ways to resist occupation;
- Emergency Contacts – Important phone numbers and resources for medical aid, evacuation, and civil defence.

The guide highlights that any information about Latvia's surrender or non-resistance should be considered disinformation and that aggressors may launch disinformation attacks through the Latvian media and carry out cyber attacks against Latvia's critical infrastructure.

The Latvian government guide is hosted on a website and can be downloaded as a reference guide. The guide itself identifies a number of Latvian government websites and social media channels that should be visited to receive up-to-date information during a time of crisis.

Lithuania

Lithuania has prepared its citizens on how to prepare for unforeseen emergencies and disasters through a public campaign – LT72. The LT72 campaign is a Lithuanian national defence/resilience initiative, focused on emergency preparedness, civil defence, and civic readiness. The number "72" refers to the first 72 hours of a crisis, emphasising the Lithuanian population's self-sufficiency and preparedness during national emergencies.

The main LT72 Lithuanian government website describes information about preparing for emergencies, e.g. having an emergency plan and having supply stocks, as well as describing the type of possible dangers that society faces, e.g. war and bombing, nuclear attacks, public disorders (Lithuanian Government, 2025).

The LT website contains static information, which is not effective in engaging with the Lithuanian public. A LT72 mobile app has been developed to make the information more interactive and relevant to citizens. The Lithuanian Ministry of the Interior developed the app to improve the preparedness of Lithuanian society for emergency situations by increasing its awareness of civic resilience and providing key information. The app itself is available on the Apple and Android platforms for free download by citizens for their mobile devices (Telsiai District Municipality, 2025). The app not only provides useful information and tests citizens' knowledge through a number of built-in tests but also features an interactive map of Lithuania with reference to the national warning sirens, collective security structures, local shelters in case of danger, and evacuation points for residents if mass evacuation is necessary. The mobile app content is available in Lithuanian and English, as shown in Figure 2. The LT72 app and national information campaign are focused on physical civic resilience and include no information in relation to disinformation or cyber security.

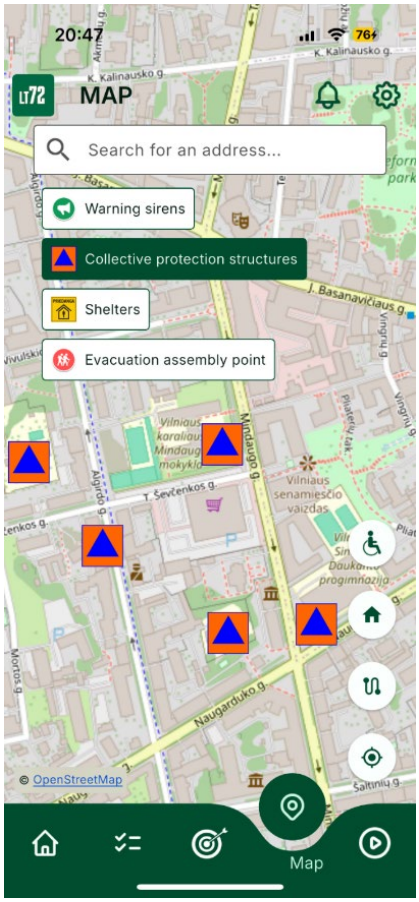

Figure 2: Lithuanian LT 72 App showing the location of community bomb shelters in Vilnius, Lithuania

In 2018 the Civic Resilience Initiative (CRI) was formed in Lithuania by a group of experts based within Europe. CRI focuses its activities on increasing the resilience of Lithuanian and other societies of the region through the means of engaging education. CRI aims to increase the resilience in the spheres of security, media literacy, disinformation, cyber, civil and grassroots activities, empowering civil societies to actively engage in educational activities with the general population (Civic Resilience Initiative, 2021).

Another recent Lithuanian initiative is the Mobilisation School, which is an online educational platform developed by the Lithuanian Ministry of National Defence in collaboration with the Lithuanian Government's Mobilisation and Civil Resistance Department. The school's primary aim is to enhance Lithuanian citizens' knowledge and preparedness regarding national defence mechanisms, focusing on mobilisation, national resilience and civil resistance strategies.

The School offers online courses, approximately one hour in length, designed to present information in a clear and accessible manner. These courses cover essential topics such as the functioning of the state's mobilization system during crises, the role of host nation support in facilitating allied forces arrival, and various forms of civil resistance that citizens can engage in. Upon completing the courses and passing the assessments, participants receive an electronic certificate confirming their accomplishment. The Mobilization School is intended for all Lithuanian citizens, regardless of age, gender, or occupation. The School emphasises the importance of collective defence readiness, encouraging every individual to understand their potential role and actions in ensuring national security. By providing these resources, the platform seeks to build a society resilient to external threats through informed and prepared society (Mobilization School, nd).

Other key examples from European countries include:

Finland

The Finnish government (Finnish National Rescue Association) has developed online resources for what Finnish citizens should do in the first 72 hours of a crisis. The resource is aimed at the first 72 hours of a crisis and, as we have seen before, in a number of Baltic countries. The guide covers natural disasters, civil defence, but also cyber security and disinformation (Finland Government, nd).

In terms of the cyber security advice, the guide's advice highlights that cyber security is essential, encompassing data protection, secure network connections (wired/mobile data, VPN), and safe user online behaviour is essential. The advice also covers considerations for citizens accessing information in terms of secure webpages, e.g. HTTPS as well as using two-step verification, strong passwords, and ensuring data back-ups of key information. The guide also advises citizens to be careful with online payments and limit their personal sharing of information on social media. Cyber awareness is highlighted as being very important, and parents should educate their children about online safety risks.

In terms of disinformation advice, the guide offers advice relating to countering disinformation such as checking the source of the information, the authors of the information, and whether the information has been verified. The advice is also not to spread disinformation and to be careful about information sources during a crisis. Social media can be manipulated, and citizens should report what they believe is questionable content or misinformation to the authorities.

The Finnish government has its guide hosted on a website and provides information that can be downloaded as a reference guide for citizens. The website itself contains a number of educational exercises so that citizen can test their knowledge of the content; the website is also linked to a number of Finnish government social media channels that amplify key parts of the guide and, in a time of crisis, would also provide additional information and real-time updates.

Poland

The Polish government (Government Centre of Security) has developed a guide called *Crisis and War Guide* (Polish Government, ND). The stand-alone guide is aimed at preparing Polish citizens on what to do in times of war and crisis. The advice includes information relating to evacuation kits, first aid, and different types of crises. The guide itself does not cover cyber security, but it does cover disinformation considerations.

The guide highlights that citizens should question whether the information they are viewing is credible and whether the information comes from more than one trusted source. Citizens should be careful not to spread disinformation that could be rumours or unverified sources/claims. In terms of a crisis, only trusted media sources, e.g. government and national media entities, should be used as sources of information.

Sweden

The Swedish government (Swedish Civil Contingencies Agency) has developed a guide *What to do in Crisis and War* (Swedish Government, 2024). The stand-alone guide is aimed at preparing Swedish citizens on what to do in times of war and crisis. The advice includes information relating to civil defence, first aid, and different types of crises. The guide itself also provides advice in terms of cyber security and disinformation.

In terms of cyber security the guide highlights the importance of being aware that cyber attacks can disrupt Swedish critical infrastructure systems and disinformation campaigns can be used to undermine Swedish society. In terms of Swedish citizens and cyber security, the focus of the guide is on cyber hygiene, e.g. creating strong passwords, not clicking on unknown links, ensuring that personal devices' security patches are updated and that citizens undertake regular back-ups of key information. The guide explains that foreign powers and others may use disinformation to influence the population, primarily through online platforms and social media. The guide also highlights that citizens should question whether the information they are viewing is credible and whether the information comes from more than one trusted source. Citizens should be careful not to spread disinformation that could be rumours or unverified. During a crisis, only trusted media sources should be used, e.g. government and national media entities should be used as sources of information.

3. Discussion

The research has focused on six European countries and the guides that they provide to their citizens on what to do in a crisis. It was intended to look beyond Europe, e.g. Australia and the USA, but it was found that these governments do not provide focused information for their citizens on what to do in a time of crisis.

The key areas to be looked at:

Legal

The legal considerations for providing information to a civilian population are extremely important, to ensure that advice in relation to security actions is in accordance with national laws and follows official government

advice. In addition, governments may be legally required to support digital literacy and public awareness campaigns as part of national cyber security strategies.

In terms of the concept of CCR (Wepner & Wester, 2015), privacy is a major focus in terms that the individual has the right to be left alone. While the state has a role in protecting citizens' privacy, individuals also bear responsibility for not divulging sensitive personal information. Looking from the institutional perspective, cyber security of civic infrastructure legislation may require reviews and updates to respond to the growing needs of current threats. The resilience testing and rapid response protocols are the obligatory requisites in any of civic infrastructure.

The European Union (EU) has implemented several legislative measures to bolster CCR, aiming to protect democratic institutions, public discourse, and societal infrastructure from cyber threats. These measures include NIS 2 Directive, EU Cybersecurity Act, EU General data protection regulation, EU Cyber Resilience Act. These legislative measures collectively enhance the EU's civic cyber resilience by establishing stringent cyber security standards, protecting personal data, and ensuring the robustness of critical digital infrastructures. The legal concepts in relation to CCR are also novel because they draw together privacy laws, cyber security and laws that are related to national security/emergencies laws. Existing laws treat these legal domains separately and not collectively which could itself pose legal challenges. Legislation designed to support CCR faces several complex challenges, especially in a fast-evolving digital environment where laws must balance security, freedom, and technological innovation. The challenges with legal regulations are also related to the cross-border jurisdiction and enforcement, fragmented legal and policy approaches**,** public awareness and engagement and economic and administrative burden. The challenges of the legal concepts are also related to the state of cyber inequity (World Economic Forum, 2024).

Disinformation / Cyber Security

The majority of the countries offer advice to citizens in relation to disinformation in terms of focusing on the quality of where information comes from, verification of information sources, and not sharing disinformation or rumors. Some countries were very specific, e.g. in Latvia, if citizens hear that the Latvian armed forces have surrendered or non-resistance is taking place, this is fake news and should not be accepted (Latvian Government 2025).

A few countries offered advice in relation to cyber security, in terms of citizens using appropriate security controls, updating their systems with security patches and having back-ups of key information.

Presentation of information

The majority of information provided to citizens took the form of static documents that could be downloaded and printed or dedicated information on web pages. It was the Lithuanian government that developed a specific apps for mobile phones. This app allows citizens, based on their physical location, to get individual information, e.g., the closest evacuation point for mass evacuation based upon a person's physical location in Lithuania.

The paper has focused on the concept of Cyber Civic Resilience (CCR) and the related information provided on disinformation and cyber security. The paper has just focused on six European countries, it is planned to expand the study in the future to include other countries beyond Europe and also new European examples, e.g. crisis guides to be sent to every French household by the end of 2025 (The Guardian, 2025).

4. Conclusion

The paper introduced the concept of Cyber Civic Resilience (CCR) and looked at how citizen focused advice is offered within six European countries. Cyber security and awareness of disinformation are indispensable for civic resilience, providing a foundation for secure, reliable, and trustworthy public services. By prioritising cyber security and disinformation awareness, communities can better withstand and recover from national crises, ensuring the continued safety and well-being of citizens, especially in these ever-changing times. The CCR concept is an older concept and needs to be updated to include cyber defence / cyber security and also disinformation to ensure that the concept is still reflective of the current global security situation and current threats and practices that countries face.

References

Civic Resilience Initiative (2021). URL: https://cri.lt/#about, accessed 17/2/2025.
Estonian Government (ND) Preparing for possible crises, URL: https://www.kriis.ee/en, accessed 17/2/2025.

Estonian Government (2022a) Cyber Security URL: https://www.kriis.ee/en/security-situation-europe/preparing-possible-crises/cyber-security, accessed 17/2/2025.

Estonian Government (2022b) What To Do In A Crisis Situation Be Prepared!, URL: https://www.kriis.ee/sites/default/files/documents/2022-10/Ole%20Valmis%202022%20ENG.pdf, accessed 17/2/2025.

European Union (2024) Tackling online disinformation, URL: https://digital-strategy.ec.europa.eu/en/policies/online-disinformation, accessed 17/2/2025.

Finland Government (nd). 72 hours how would you cope on your own, URL: https://72tuntia.fi/en/, accessed 17/2/2025.

Latvian Government (2025) 72 Hours: What to do in a crisis, URL: https://www.jelgava.lv/wp-content/uploads/2023/06/72hours.pdf, accessed 17/2/2025.

Lithuanian Government (2025) Why LT72?, URL: https://lt72.lt/, accessed 17/2/2025.

Telsiai District Municipality, (2025) Mobili programėlė LT72 padės gyventojams geriau pasirengti ekstremaliosioms situacijoms, URL: https://telsiai.lt/naujienos/mobili-programele-lt72-pades-gyventojams-geriau-pasirengti-ekstremaliosioms-situacijoms?disabilities_action=disable&lang=lt, accessed 15/3/2025.

The Guardian (2025) France preparing 'survival manual' for every household, report says, URL: https://www.theguardian.com/world/2025/mar/18/france-preparing-survival-manual-for-every-household-report-says, accessed 19/3/2025.

Mobilization and Civil Resistance Department under the Ministry of National Defence of the Republic of Lithuania. ND), URL: https://mobilizacijosmokykla.lt/, accessed 15/3/2025.

Polish Government (ND). Crisis and War Guide, URL: https://www.gov.pl/web/rcb-en/crisis-and-war-guide, accessed 15/3/2025.

Swedish Government (2024) In case of crisis and war, URL: https://rib.msb.se/filer/pdf/30874.pdf, accessed 15/3/2025.

Wepner, B & Wester, M (2015) Towards a Better Understanding of Cyber Civic Resilience (CCR). in J Beyerer, A Meissner & J Geisler (Hrsg.), Security Research Conference - 10th Future Security Proceedings. Germany.

World Economic Forum (2024). Global Cybersecurity Outlook 2024, URL: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf?bcs-agent-scanner=3d6200b9-6784-8640-a1fa-bd235ef7292d, accessed 15/3/2025.