friends of europe

SUMMER 2022

21st century warfare: a whole of society approach to resilience

EVENT REPORT

Cover image credits: cottonbro from Pexels

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the European Union

Co-organised with

This report reflects statements and questions made during a one-hour debate hosted by Friends of Europe on 1 June 2022. The event was held following Russia's invasion of Ukraine, in response to security questions raised by an increase in both military activity and social interaction online.

Ukraine has been enduring a conventional attack by Russia since the annexation of Crimea in 2014. The latest invasion was justified by Putin based on a false narrative, spread and fuelled by strictly controlled state media in Russia, disinformation campaigns by Russian media outlets, as well as the Kremlin's interference in other countries' elections.

In response to Russia's latest aggression against Ukraine, we are witnessing a global whole-of-society response that involves not only state and institutional actors, but an unprecedented level of support and influence from private companies and citizens. Instead of facing an isolated Ukraine, Russia is faced with a united West and an army of hyper-enabled private citizens, civil society groups, NGOs and companies challenging it in the information sphere and cyberspace, and by providing key capabilities to Ukrainian forces.

This new global swarm is tracking Russian troops, hacking Russian infrastructure, debunking disinformation and trying to reach out to the Russian population to inform them about the war. Local organisations in neighbouring states are arranging support for Ukrainian refugees.

At the same time, the staying power of member states' societal resilience remains fragile in the aftermath of the pandemic and during a time when citizens were expecting their lives to return to normal. For these and many other reasons, strengthening ties and understanding between governments, local authorities, the private sector and citizens remains of vital importance as the conflict in Ukraine continues and we look to a future that includes the greater use of AI, the dawn of augmented and virtual reality, and their ability to amplify disinformation campaigns leading to radicalisation and disinformation-driven violent extremism.

Speakers and participants considered questions including:

- What are the implications of so many non-state actors supporting Ukraine against Russia's aggression?
- Which synergies and forms of cooperation between governments, local authorities and the private sector can be established to ensure whole-of society efforts remain effective and do not act against member state intentions?
- Is it time to update the Geneva Conventions to address cyberspace and the expanded role of private actors in conflict?
- How can governments build trust to avoid hyper-empowered private actors susceptible to disinformation to turn on them and/or become radicalized?

The debate was part of Friends of Europe's Security briefing series.

Recommendations

Discussion focused on the challenge of regulating a situation that is in constant flux – in many cases, using rules and standards developed almost a century ago. Five key themes emerged to guide citizens and policymakers looking for ways to understand and address the challenges of war in the 21st century world.

1 **Build resilience at all levels**

2 **Foster a whole-of-society approach**

3 **Develop a Geneva Convention for cyberspace**

4 **Educate through change**

5 **Face challenges, embrace opportunities**

Resilience at all levels

Resilience has in recent years become almost a label that can be attached to any situation, particularly in EU debates. Resilience is something everyone aspires to and that seems relevant in most areas. This could mean financial resilience after the 2008 banking crisis, societal resilience after terror attacks around Europe or climate resilience.

Energy and food resilience are now high on the agenda, not just in Europe but around the world, as citizens and governments suffer from the aftershocks of war in Ukraine. As society moves to operate in new domains, be it outer space or online metaverses, we need to consider how different environments. Back on earth, resilience against fake news and online disinformation becomes a greater challenge every day.

> “ Are we becoming more resilient? Are we coordinating well at various levels? Are we bringing all actors around the table to a frank conversation about what we are doing well and what badly?
>
> **Jamie Shea**, Senior Fellow for Peace, Security and Defence at Friends of Europe and former Deputy Assistant Secretary General for emerging security challenges at NATO

With all this in mind, participants considered whether or not lessons learned about resilience in one sector, such as banking, are applied across others. “Are we becoming more resilient?” asked event moderator **Jamie Shea**, Senior Fellow for Peace, Security and Defence at Friends of Europe and former Deputy Assistant Secretary General for emerging security challenges at NATO. “Are we coordinating well at various levels? Are we bringing all actors around the table to a frank conversation about what we are doing well and what badly?”

The public and private sectors could be better integrated through joint exercises, including military exercises. Conducting public-private risk assessments and joint exercises would help to build resilience and communities of interest. Governments’ first reaction is often to compel the private sector to act, which too often scares away the private sector. Conversation with citizens and private sector representatives would better protect the public interest.

The private sector is increasingly becoming an ‘impactful layer’ of society, said a participant, “but trust doesn’t always exist here. We need to think about how we can better engage with the private sector.”

A whole-of-society approach

The horror of war brings social resilience to the fore, with people trying to reorganise societies to welcome and shelter refuges and their children. This leads to questions about what countries can do alone and what requires a broad sharing of capabilities, as well as about the need for resilient citizens within resilient states. For all of this to be possible, trust and collaboration are needed at all levels of society.

"People will want to protect a society they believe in, one in which they feel equal partners," said **Chris Kremidas Courtney**, Senior Fellow for Peace, Security and Defence at Friends of Europe. This has been clearly shown in Ukraine, where people have rushed to fight for a democracy and civil society that they only recently built for themselves.

In building a society, through for instance the creation of a Supreme Court, Ukrainians also built trust and a shared societal cause. This has spilled over into strong civil society support for Ukraine from neighbouring countries such as Poland, Georgia and Latvia.

> "In past wars, people watched powerless, today, they have the ability to reach out and have an impact
>
> **Chris Kremidas Courtney**, Senior Fellow for Peace, Security and Defence at Friends of Europe

Ukrainian success in the cybersphere – an area that was previously seen as a Russian strength – has empowered citizens. By recording and sharing experiences and events online, ordinary people have been able to send stories around the world. They have in the process also made it very easy to collect information about potential war crimes.

"In past wars, people watched powerless," Kremidas Courtney said. "Today, they have the ability to reach out and have an impact."

The mobilisation of civil society online has seen a speed of response in which individuals and private actors have outstripped governments. Moving outside of traditional government or corporate hierarchy, a sense of moral obligation and outrage has been allowed to fuel swift action.

Following Russia's invasion of Ukraine, rather than seeing solidarity only from the familiar big players, like NATO, the United Nations and the EU, private businesses were able to quickly make a difference. This has been seen through donations of money and equipment. It has, however, also raised concerns about how easily private businesses may be influenced by targeted disinformation.

A Geneva Convention for cyberspace

This new style of warfare needs new treaties to redefine roles and protect people as war moves to the cybersphere. This means new rules of engagement for digital conflict.

"A sort of Geneva Convention for cyberspace is needed," said **Hanna Linderstål**, CEO and Founder of the Earhart Business Protection Agency. An updated treaty would help society manage a new era of digital warfare that was unimaginable when the original Conventions were drafted between 1929 and 1949. "What is a combatant? What is an unacceptable target? What can we accept in a cyberwar? That all has to be discussed and perhaps even decided on," Linderstål explained.

Other participants agreed that it was time to take a hard look at an update of the Geneva Conventions. This could mean, for instance, rethinking the definition of roles

and responsibilities in conflict. The same person working as an engineer behind a keyboard in Antwerp could be an international computer hacker or a combatant in a war on the other side of the world.

With no 'cyber-attack guidebook' to direct our actions and reactions, there are no longer any clear answers about what constitutes an act of war. A supply chain could as easily be disrupted by a vendor's mistakes or bad habits as by a hostile attack.

"We need to do a better job of understanding the sheer complexity of what we're seeing," said Shea. "We have to learn as things are happening. Warfare is changing. Who is a warrior? What are the rules of engagement?"

> "A sort of Geneva Convention for cyberspace is needed. What is a combatant? What is an unacceptable target? What can we accept in a cyberwar? That all has to be discussed and perhaps even decided on
>
> **Hanna Linderstål**, CEO and Founder of the Earhart Business Protection Agency

A new cyber-Geneva Convention would also need to address the impact that online disinformation can have on troops and citizens. Participants considered the possibility of a hostile force using social media and fake news to disrupt chains of communication or command, potentially leading combatants to attack their own forces.

Educating through change

Participants throughout the hour-long event stressed the need to educate decision-makers and schoolchildren in the new realities of 21st century warfare. The increasing complexity of the existing and emerging online worlds was given as a major challenge to developing education programmes.

"People are super-afraid of complexity. They are either frighted or they tune out," said a participant from a public international organisation. "We need to invest more in understanding." He warned, however, against trying to fix one secure policy position, particularly when it comes to resilience and education, quoting Princess Leia in Star Wars: "The more you tighten your grip, the more star systems will slip through your fingers."

Giving people a basic education through at least generic guidance would be a helpful start, as long as citizens and policymakers accept that there will be disruptions and failures along the way. If consumers are taught not to be afraid and to understand what they are seeing, even a steady stream of different sources of information can promote social resilience.

Modern technological warfare, like all cyber-technology, is in a constant state of flux. The average European adult today already spends 11 hours online. New immersive technologies, including augmented reality glasses, are likely to be on the market next year.

"For the average military commander, the situation is always getting more complicated and sophisticated," said a participant from a European institution. Modern military uniforms already rely on complex IT systems.

Military training for young soldiers almost certainly needs to include an understanding of cyber-security, alongside traditional strategic and technical training. There have been several cases of military units being traced by tracking the cell phone activity of soldiers on operations – or even by examining photos of soldiers' boots posted on social media.

The search for simple answers can lead to the creation of closed groups, in which members shut themselves off from other sources of information. People should instead know how to be smart online and not afraid of social media. This starts with teaching schoolchildren how to search online safely and continues through educating military troops, as well as their leaders.

Facing challenges, embracing opportunities

Europe is now in a relatively strong position, in terms of understanding and critical thinking about the cybersphere and 21st century warfare. Over the coming years, there will be difficult decisions to make and complex conversations to have with governments and members of parliament, including the European Parliament.

Educating decision-makers will be part of this process, and so will upgrading our own core operating systems. In many cases, critical hospital infrastructure was found to still be using Windows 95.

More generally, people need a basic understanding of how the grid works, if they are to understand how modern healthcare systems and even buildings function. This can help everyone to identify and guard against vulnerabilities. As well as educating humans, there needs to be a better use of technology to protect technology itself, for instance, by finding ways of using AI to detect false claims online.

When it comes to online activity in the face of war, there is a groundswell of mobilisation. We are at a historic moment in the development of social resilience. "Is anyone mapping this?" asked a participant from academia.

The more we digitalise our societies, the more we need to think about cyber-security. There are many things that could be done to promote cyber-security that aren't done today because of a lack of basic understanding. We are all still learning.

Friends of Europe
Connect. Debate. Change.

info@friendsofeurope.org
friendsofeurope.org

Friends of Europe is a leading think-tank that connects people, stimulates debate and triggers change to create a more inclusive, sustainable and forward-looking Europe.