WINTER 2018

BUILDING AND FOSTERING RESILIENCE

REPORT

This report is part of Friends of Europe's Peace, Security and Defence Programme supported by the United States European Command (EUCOM). Our work is firmly anchored in our expertise in a range of fields, including energy and climate change, geopolitics, international development, migration and health. We seek a holistic approach to European, transatlantic and global security policies. Security considerations are, in turn, mainstreamed into these areas of expertise, enriching the debate by encouraging experts to think outside their comfort zones.

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
Europe for Citizens Programme
of the European Union

Image credits: Cover photo, p40: teamjackson/Bigstock, p6:pudiq/Bigstock, p10: Benny Marty/Bigstock, p16: AlexRotenberg/Bigstock, p20: encrier/Bigstock, p26: weerapat/Bigstock, p30: shutter2u/Bigstock, p36: Rawpixel.com/Bigstock

TABLE OF CONTENTS

FOREWORD

Resilience has become a key word in any discussion of modern day security challenges, and it captures two essential realities that our increasingly complex and urbanised societies need to acknowledge and confront.

Shocks to the system will be more frequent and potentially more destructive because we are multiplying rather than reducing our vulnerabilities. From airlines to train stations, pop concerts and even pedestrians walking along bridges, terrorists can attack with relative ease. If they cannot manufacture high tech explosives, they can have recourse to hired cars and trucks and even kitchen knives. These types of attacks are impossible to anticipate and, through attracting significant media exposure, encourage emulation by future terrorists. Increasingly networked communication systems, digitalised critical infrastructure and globalised supply chains present multiple choke points and attack surfaces that can be exploited.

In addition to these familiar, man-made resilience challenges, catastrophic black swan events caused by severe weather conditions, disasters or pandemics can easily spiral out of control and move across continents in a matter of days. We have seen how an unprecedented series of four hurricanes in a row has crippled governments, economy and communities on several Caribbean islands last year. We have had close shaves with diseases such as Ebola, SARS and MERS, and lest we forget humanity's vulnerability to disease in a year that marks the centenary of the great Spanish influenza of 1918 which killed at least 50 million people, five times more than the Great War.

Our increasing vulnerabilities can be exploited by a multitude of actors. Anyone from anywhere can launch virtual malware into our computer systems. Non-state actors such as ISIL or Al-Qaeda can acquire chemical weapons and ballistic missiles. Moreover, even very weak states can challenge our security by acquiring niche capabilities, as demonstrated by North Korea when it launched its WannaCry cyberattack against governments, companies and public health systems in 2017.

Resilience will be a leading concern for the European Union and NATO for many years to come.

We need to constantly map our vulnerabilities and work hard to better understand the interdependencies of our critical infrastructure. This requires both timely decision-making by the governments that withstand these breakdowns and a high degree of cooperation between key actors. We need to go beyond crisis management: we need to reduce our vulnerability by hardening our critical infrastructure, upgrading the standards of our IT networks, and improving and educating our response teams and ensuring the continuity of government services.

The key lesson is that resilience can be strengthened. Good planning, organisation, exercises, sharing best practices and developing the right capabilities can save lives, lessen the impact of attacks and speed up recovery. In recent times, the EU and NATO have prioritised resilience in their agendas and have improved their cooperation, particularly in the areas of cybersecurity and countering hybrid warfare. Yet, to achieve a truly holistic approach to resilience requires maintaining a dialogue between these two institutions as well as civil society more broadly.

Friends of Europe has been able to bring its voice to this debate by organising three timely and relevant events this year: on urban resilience and cities' response to terrorism, on building climate resilience and on fighting back cyberattackers. The report that follows captures the key contributions from these important debates and points the way forward for both policymakers and industry and civil society representatives. The report does not claim to be exhaustive – how could it be on such a diverse subject? – but it does provide many valuable insights and shows how European and global resilience can be improved if we have the necessary political will as well as the time, effort and resources in place.

Happy reading!

Jamie Shea,
Senior Fellow at Friends of Europe

POLICY RECOMMENDATIONS

BUILDING URBAN RESILIENCE

Put in place robust and strategic urban planning: Architects, urban planners, engineers, and urban sociologists should be consulted in designing and implementing physical preventative measures against terrorism. This is to ensure that a holistic and smart approach is taken to urban planning which maximises safety whilst ensuring that the general public does not live in fear of potential threats.

Strengthen critical infrastructure at the local level and ensure effective information sharing: In order for a city to respond effectively to a crisis, it must ensure that its emergency services have the same command-and-control structures set in place for a range of situations. The resilience of these systems is reinforced by ensuring effective information sharing across emergency services as well as between the public and private spheres. Responses to an attack can therefore be more efficient and prevent bottlenecks in emergency-response infrastructure, including hospitals.

Encourage engagement with multiple actors and build private-public partnerships: The private sector is encouraged to participate in building resilient cities. Considering the depth of expertise companies have in mapping and analytics, public-private partnerships are encouraged in order to improve planning and prevention and facilitate faster and more efficient responses. It is however important that such analytics are handled in the most sensitive way possible to ensure that the data is not used for purposes which go beyond its reach. Finally, private organisations and companies should consider supporting community-led programs which seek to promote societal and community inclusiveness.

BUILDING CLIMATE RESILIENCE

Build resilience through early-warningand foresight capabilities: To meet the needs of a changing environmental security landscape, greater foresight capabilities are needed to predict and prepare for the diverse impacts that climate change will have on security. Although governments cannot prevent natural hazards such as hurricanes or earthquakes from happening, they can help bridge humanitarian relief and long-term development efforts to protect vulnerable populations. This can include building better and improved water and sanitation systems or using science-based information about emerging climate threats can be used to reduce risk and improve resource allocation at the time of impact.

Recognise climate change as a non-traditional security threat in policy: Understanding and recognising climate change as a security threat means understanding security in the 21st century. By recognising climate change as a non-traditional threat or at least as a threat multiplier, enables governments and the NATO Alliance to build emergency responses to extreme weather events, and to adapt military planning, training and budgeting accordingly. Although institutions such as NATO have already engaged in developing policy and conducting operations responding to the impact of climate change, a more concrete approach is needed. This can include a faster process of sharing climate change-related information between member states and NATO or build from national capacities for dealing with climate risks to the NATO level. NATO members should develop a common strategy on how to integrate the mitigation of climate risks into their national defense strategies.

Improve urban infrastructure focused on collective territorial governance : Urban infrastructure and urban networks need to be adapted to respond to the risks threatening them, including heat waves, major floods, intense rainfall events and frequent pollution peaks. At the forefront of climate change risks, cities must manage and evaluate the infrastructure in place in an integrated way and ensure their resilience. Mobilising and training of a wide range of stakeholders, and producing additional spatial data on the territory, its vulnerabilities and the risks that threaten it, are some of the drivers that will enable a better allocation of resources and ensure the implementation of shared and sustainable solutions.

Mobilise the private sector to develop risk management solutions: More companies should develop climate resilience solutions that would help protect customers from a range of climate risks. These include resilient building materials and services; new

BUILDING CYBER RESILIENCE

Invest in digital education and training: Building a strong EU cyber skills base is part of the European Commission's Cyber Strategy with the aim of empowering citizens to fend off cyber threats at every level. This requires developing cyber training of the workforce, additional cybersecurity training for tech specialists and introduce new specific cybersecurity curricula. The goal is to ensure that it becomes natural to design digitally connected products which incorporate and respect security standards from the very beginning. Better cyber hygiene needs to be adopted by individuals, businesses and organisations.

Create a market for "security-by-design" products: The private sector can play an important role in helping the European Commission in its implementation of an EU cybersecurity certification framework. A "security-by-design" approach could be used for connected devices to ensure that cybersecurity is addressed before any product is put on the market. Initiatives such as the EU NIS Directive, the GDPR and NATO's Cyber Defence Pledge have important roles to play here. This would benefit businesses as well, as they would avoid going through several certification processes. Ultimately, this new labelling system will incentivise the creation of more resilient networking and cyber solutions such as stronger encryption.

Apply international law in cyberspace: While cyberspace has often been referred to as a "jungle" or the "Wild Wild West", clear international cyber norms do exist and have been developed throughout the process of the UN Group of Governmental Experts (GGE). It is important that the normative framework for cyber behaviour is respected and needs to be implemented. In this context, the Tallinn Manuals serve as an important framework for Governments to follow. While legal definitions are crucial, attempts to establish a global convention of some sorts on cybersecurity are likely to get bogged down for years, so small scale or sectoral approaches are important parallel measures to take.

Protect critical infrastructure: Attacks on critical infrastructure, like the WannaCry and NotPetya attacks, demonstrate the devastating effect of malicious assaults. In order to improve their critical infrastructure resilience strategies, states need to refine and implement industry standards for cybersecurity in IT and banking systems, government services, the military, utility providers including energy and telecom companies, hospitals, transport enablers such as air traffic control and navigation systems, and so on. If resiliency measures are robust and publicly known, then it may have the effect of persuading malicious actors that their cyberattacks are unlikely to have the devastating effect they wish to inflict.

PART 1 I TERROR AND THE CITY

BOOSTING URBAN RESILIENCE TO VIOLENT EXTREMISM

INTRODUCTION

Building resilience is about ensuring that the capabilities, procedures and measures that enable a country's institutions to act in a flexible manner in case of a major shock are in place. In recent years, many of the world's major cities have had first-hand experience dealing with the prevention or aftermath of deadly terrorism. While they are getting better at combatting and responding to attacks, countering the evolving threats requires further coordinated worldwide action, panelists told a Friends of Europe Policy Insight "Terror and the city: boosting urban resilience to violent extremism" on 22 February. How can cities reinforce their resilience or their ability to respond, persevere and adapt to internal or external crises? Their ability to survive and adapt to shocks – whether a terrorist attack or other – depends on the robustness of a good governance framework at the local, national and international levels.

"If you have hundreds of bespoke plans for every scenario, nobody gets that plan out in the case of an emergency. So we have one"

Paul Argyle
Strategic Advisor to the Mayor
and Deputy Mayor of Manchester

A LOCAL LEVEL RESPONSE BASED ON EFFECTIVE PLANNING AND MULTI-STAKEHOLDER TRAINING

Fundamental to urban resilience is a city's capacity to respond, and to be able to handle attacks in the quickest and most effective way possible. According to Paul Argyle, Strategic Advisor to the Mayor and Deputy Mayor of Manchester, this is done by starting on the basis of a "generic response". He talked about the widely-praised reaction to an attack in May 2017, when a terrorist bombed the Manchester Arena, killing 23 people including the attacker. "If you have hundreds of bespoke plans for every scenario, nobody gets that plan out in the case of an emergency. So we have one. We use the same plan when we respond to an incident, so that we have the same command-and-control structures. We then support that with plans for specific scenarios."

Central to Manchester's response was the involvement of a broad range of agencies that often work together. "When we're in a command-and-control room, quite a lot of us in the room have met each other and there's a common understanding and trust across all the many agencies," said Argyle. "It isn't just the emergency services and the military. It's local authorities and utilities – the private and public sector coming together and then exercising." As a result, in 2017 casualties were taken to different hospitals where there was sufficient capacity to treat them, with only one person needing to be transferred to a different hospital from the one they arrived in.

Another factor was a mass fatality plan, he said. “You need to get those people with dignity to a place where they can be identified. It is important to have a plan for disaster victim identification. The families want to know within minutes.” The city’s mortuary plans were used again this winter, when there was an outbreak of influenza.

STRENGTHEN RESILIENCE TO ATTACKS WITH STRATEGIC URBAN PLANNING

Recent trends in violent terrorist attacks have presented cities with a dilemma: if they take stringent measures to combat attacks, they will be disrupting city life – which is the goal of the terrorists; but if they don’t do enough, they will be accused of negligence if an attack does take place.

> **“In response to increasingly sophisticated ways of targeting terrorists, they are using means that are not as easy to detect”**
>
> **Dharmendra Kanani**
> Director of Strategy at Friends of Europe

The 2016 attack in Nice, when a truck was deliberately driven into crowds of people, killing 86, showed the difficulty of dealing with attacks using vehicles. “In response to increasingly sophisticated ways of targeting terrorists, they are using means that are not as easy to detect, such as low-tech, low-key vehicles,” said moderator Dharmendra Kanani, Director of Strategy at Friends of Europe. “What do we do to protect communities? How do we create that bounce-back factor?” he asked.

A few years ago in Pristina, 25,000 people gathered for a beer festival in the main square. A fight broke out between two young men, one of whom fired a gun. Many in the crowd thought a terrorist attack was occurring and tried to run away. Forty people were injured in the resulting stampede. The mayor, Shpend Ahmeti, cancelled the festival for the next three nights. “I was criticised heavily for causing paranoia in the public,” he said. “They said: ‘You should have gone on.’ But my fear was that we didn’t have the necessary responses in place – not just for attacks but also for pranks.”

As demonstrated by Nice or Berlin, attacks can be carried out with very basic equipment. “It doesn’t require a bomb anymore,” said Ahmeti. “It takes one truck, which is very easy to get, and anyone can be a driver. I think the biggest problem we are facing in cities is the change of terrorist attacks from what we have known as ‘hard targets’ – government institutions and buildings with economic importance – to ‘soft targets’, such as crowds in open spaces. These attacks are meant to cause fear and paranoia in the general population.”

One way to hamper attacks is to adapt urban design by placing physical barriers to restrict access to pedestrian areas. City authorities are hiring architects to build structures that would be unnoticeable to the general public, but will restrict access to motorised vehicles at the most vulnerable points. “The biggest challenge for me is to find a balance between acceptability and safety: not causing paranoia but at the same time doing beautiful and safe urban design,” explained Ahmeti.

HARNESSING NEW TECHNOLOGIES

Drones are often talked about as a threat because of their potential for offensive use. But technology company Nokia is developing ways to use them for disaster recovery through its Nokia Saving Lives initiative, which provides communications technology and technical-expert assistance to emergency response teams. For example, drones – combined with applications such as video streaming, gas sensing, mapping, and analytics – enable Nokia to help rescuers rapidly gain situational awareness so that they can provide the fastest possible response. “We are looking at how a fleet of drones could efficiently identify people in a disaster area,” said Emmanuelle Pierrard, Head for Energy, Transport and Public Sector at Nokia Benelux.

The company is also investing in video and data analytics that could be used to spot an anomaly in a crowd, so that security forces could then act to prevent an attack. “We are working on a lot of innovations to reinforce public safety networks,” said Pierrard. “If the police or a law-enforcement agency is looking for a suspect car, we can integrate all the devices to push some video information to a control centre and then perform analytics on information gathered by those cameras.” Pierrard highlighted the data privacy aspect attached to this: “We make sure that the video analytics is done on the premises, so it does not need to travel on the Internet before being analysed. And we can mask background information that is not relevant to what you are looking for.”

> **“The biggest challenge for me is to find a balance between acceptability and safety: not causing paranoia but at the same time doing beautiful and safe urban design”**
>
> **Shpend Ahmeti**
> Mayor of Pristina

STRENGTHEN NATIONAL SECURITY AT AN EU LEVEL

Government structures are critical. European Union initiatives such as the Schengen Information System (SIS) have improved their ability to track potential terrorists. Maintained by the European Commission, the SIS is used to find information about individuals and entities for the purposes of national security, border control and law enforcement. These systems faced criticism after the terrorist attacks in Paris and Brussels.

“We were accusing the European Union of all sorts of things,” said Camino Mortera-Martinez, a Research Fellow at the Centre for European Reform. The accusations ranged from a lack of support to the Member States, not monitoring the influx of refugees and migrants to Europe from conflict zones who later committed acts of terrorism (i.e. the 2015 Paris attacks), or the inability to stop French citizens from going to Syria. Some of these accusations were legitimate, such as the deficiencies in the functioning of the Schengen Information System. The so-called Article 36 alerts on suspicious people were not working properly.

> **“If the police or a law-enforcement agency is looking for a suspect car, we can integrate all the devices to push some video information to a control centre and then perform analytics on information gathered by those cameras”**
>
> **Emmanuelle Pierrard**
> Head for Energy, Transport
> and Public Sector at Nokia Benelux

However, in the last two years or so, many of these faults have been repaired, said Mortera-Martinez. “The European Union has got its house in order. We now have amended the Schengen border codes. We now have a better approach to asylum and immigration and how to identify people. We have also improved the way the Schengen Information System works.”

Still, implementation of many aspects of these systems is the responsibility of individual Member States, some of whom are reluctant. “The EU can ask Member States as much as they want to input this kind of information. But if they are reluctant to do it because they don’t trust their counterparts, then we’re going to be in the same situation as we were when Salah Abdeslam and his friends went back and forth between Paris and Brussels undetected. There is a case, not for more Europe, but for a better Europe – for a Europe that actually supports Member States in the things they need to be supported in.” This support would allow governments and their local communities to focus their time and resources on countering and preventing violent extremism efforts and urban planning. The EU can still support these initiatives through financing methods, but it cannot propose top-bottom measures when a bottom-up approach is needed.

ROR AND THE CITY
BAN RESILIENCE TO VIOLENT EXTREMISM
#FoEDebate

OR AND THE CITY
BAN RESILIENCE TO VIOLENT EXTREMISM

DESIGNING PROPORTIONATE SECURITY RESPONSES TO 'SOFT TARGET' TERRORISM

A contribution by Jon Coaffee is Professor of Urban Geography at the University of Warwick and Director of the Resilient Cities Laboratory

Recent attacks in Berlin, Nice, Stockholm, London, New York, Melbourne and elsewhere had at least one thing in common: each used fast moving vehicles against crowded public spaces; 'soft targets' which are relatively open to attack due to their easy accessibility and high crowd density.

This has led to a re-evaluation of security in many public locations. In attempting to limit the occurrence and impact of such attacks, urban designers and security experts have, to date, primarily established measures that reduce vehicular access to public spaces and have sought to maximise the 'standoff' distance between the road and 'target' locations.

The techniques that have traditionally been applied to public spaces have largely been based on policing or military-style approaches that seek to secure access to risky locations through robust physical interventions. Such approaches are similar to commonly understood planning interventions such as Secured by Design or Crime Prevention through Environmental Design. They seek to make spaces safer through the manipulation of the built environment in ways that reduce the attractiveness and physical access to targets.

Most common amongst such initiated interventions have been 'barrier' methods of protective security: crash-rated security barriers, steel bollards or simple temporary concrete or wooden blocks, all of which are intended to limit vehicular access to public places. However, such a 'one-size-fits-all' approach to securing the public realm is seen by many as disproportionate due to its impact on the liveability, walkability, character and accessibility of public spaces.

In response to such challenges, a number of countries or cities – notably the United Kingdom, the United States, Australia, and Abu Dhabi in the United Arab Emirates – have advanced strategic planning and design guidance on how planners and other built environment stakeholders can respond to terror attacks in crowded locations.

Most common amongst such initiated interventions have been 'barrier' methods of protective security

Such guidance argues this should be done through embedding security into design plans in ways that reflect upon and turn threat information into effective, protective security measures. This should be considered at the earliest opportunity within a design process, and should be proportionate with the level of risk faced.

However, until recently, in practice, and faced with an escalating threat of urban terrorism, this has meant the ubiquitous use of security bollards or crude barriers, combined with high-visibility policing.

After recent tragic instances of vehicle-based terror attacks, cities have once again looked to bollards and barriers for protection. In many locations, these have been placed around key sites to stop further attacks or to reassure the public that the threat of terrorism is being taken seriously; as a display of 'security theatre', as some might call it.

But is it possible, then, to put effective counter-terrorism measures in place without changing how we use and feel about our urban centres? How can subtler landscape alterations and the innovative use of street furniture become the go-to option instead of obtrusive security features?

Reimagining a public realm improvement that seamlessly incorporates security requires that innovative thinking is applied in the design process. For example, can street furniture provide additional benefits and be designed to serve the purpose of protection, whilst adding an aesthetic or functional dimension to public space beyond its role in safety?

In a small number of locations, security features have been increasingly camouflaged and subtly embedded within the cityscape. Examples of such 'stealthy' features include balustrades or artwork erected as part of public realm improvements or hardened benches, lampposts, planter pots or other streetscape elements. These still fulfil the purpose of "hostile vehicle mitigation", with designs capable of stopping a seven-ton truck traveling at 50 miles per hour (80 km/h). Road design alterations, such as chicanes, have also been used to reduce the speed of vehicles traveling to a target location.

The look and feel of our public realm is important

After recent vehicle attacks, alternatives to bollards are now being contemplated in a number of places as part of a desire to maintain an open and accessible city. In some locations, notably Milan and Melbourne, this has led to concrete blockers being decorated by protesters as a way of demonstrating against the imposition of security 'eyesores'. There has been greater engagement in a number of cities with the artistic and cultural community with regard to designing alternative security interventions that reduce the appearance of security whilst keeping the city as vibrant and accessible as possible.

The look and feel of our public realm is important. How our public places are designed tells us a lot about the type of society we are and the type of society we would like to be. We live in dangerous times but how we react to the risk of terrorism will have an impact on our public areas and civic sense for many years.

In many ways, the threat to cities comes as much from our policy responses to such risks as the actual act of terrorism. In this sense, providing prescriptive guidelines on protecting against terrorism in public places is a difficult task, especially in societies that value freedom of movement but are seen as under threat of attack. Whilst ongoing urban revitalisation has increasingly emphasised the quality of life, this now sits uneasily beside concerns to "design-out" terrorism, as security becomes an integral part of the design process.

In responding to terrorism we should not let exceptional security measures become the norm. Put simply, bollards are not enough. We need to think inventively about how we can secure public spaces effectively whilst retaining the essential characteristics that make them accessible, friendly, walkable and welcoming places that are attractive, sustainable – and safe.

CAMBRONNE
PT DE BIR-HAKEIM
TROCADÉRO
CONCORDE

PART 2 | BUILDING CLIMATE RESILIENCE
COOPERATION, COLLABORATION AND FORESIGHT

INTRODUCTION

States and communities around the world are increasingly being confronted with a variety of climate change and security-related challenges. Building resilience in the emerging and evident nexus between climate and security was a key discussion point throughout the Friends of Europe Policy Insight "Building climate resilience: cooperation, collaboration and foresight" on 24 April. Environmental pressures are a special challenge in that their consequences can be disastrous for communities and states, leading to disruptions in food, water and energy supplies and damages to critical infrastructure. These in turn pose risks to the social and democratic order more broadly, which can amplify instability and insecurity in cities and countries.

While climate action has been a priority for years, the international community has struggled to create a concrete, large-scale blueprint for preparing for and mitigating such threats and challenges. Absorbing and adapting to these threats, while in parallel mitigating them, will require better and improved governance and a system-wide shift in our attention to provide more funds, resources and expertise to strengthen disaster risk management, risk reduction and preparedness.

> **"Climate change is fundamentally redrawing the maps of the world and that is going to have a massive impact on society, on politics, on people and on communities. It is redrawing where rain falls, where food can be grown, where people can live and where maritime borders go"**
>
> **Oli Brown**
> Senior Programme Coordinator
> for Disasters and Conflicts at the UN
> Environment Programme (UNEP)

CLIMATE CHANGE AS THE NEW SECURITY THREAT

Climate change has become increasingly embedded within the international security discourse. The adverse effects of climate change on natural, societal and governance systems certainly amount to a threat that is transnational in scope. "Climate change is fundamentally redrawing the maps of the world and that is going to have a massive impact on society, on politics, on people and on communities. It is redrawing where rain falls, where food can be grown, where people can live and where maritime borders go," said Oli Brown, Senior Programme Coordinator for Disasters and Conflicts at the UN Environment Programme (UNEP).

The nexus between climate and security is increasingly evident said moderator Dharmendra Kanani, Director of Strategy at Friends of Europe: “Climate change is the new security threat – or at least it feels like that.” Climate change intersects with poor environment management and broader institutional or socioeconomic fragility such as racial discrimination, and therefore multiplies existing threats to create significant political issues. However, this makes the security impact of climate change often hard to grasp; primarily because it is not a security threat in the sense of having a clear enemy, which means that there is no conflictual relationship that you can deal with.

BUILDING RESILIENCE THROUGH EARLY-WARNING AND FORESIGHT CAPABILITIES

Climate change is different from many other problems because it is evolving fast. However, a lack of foresight and prevention by policymakers exacerbates the efficient implementation of solutions. Typically, once a problem is located, a solution is designed and then implemented. However, that takes too long for problems related to climate change, and the solutions rapidly become out of date. “Now we need to think about how the world is going to be,” said Brown. “The world is going to be a different place to how it is now, not only because of climate change, but because of a whole range of other things. 60% of the buildings that are going to exist in 2050 haven’t yet been built.”

“How can we make use of the available science to be smarter in how we respond?”

Tessa Kelly
Climate Change Coordinator at the International Federation of Red Cross and Red Crescent Societies (IFRC)

A changing climate is intensifying work for humanitarian organisations around the world. In the face of mounting environmental pressures, science-based information about emerging climate threats can be used to reduce risk and improve resource allocation. “We have to become more anticipatory, more forward-thinking and smarter in our approach,” said Tessa Kelly, Climate Change Coordinator at the International Federation of Red Cross and Red Crescent Societies (IFRC). One tool that the organisation is working on is forecast-based financing, which uses climate science forecasts and implements early action ahead of disasters and extreme weather events. This favours a preventative approach which would be more efficient than requesting financing after the impact of a disaster. The organisation is also working with communities to better understand the risks they face. Taking a community view would improve the capacity and capability of agencies to build resilience.

Supported and encouraged by the German government, the IFRC is currently working on financial mechanisms to enable this. The aim is to use forecasts that will enable triggers to be identified so that funding can be released, and food, water and hygiene kits can be distributed ahead of the impact. In 2017, for example, Cyclone Mora caused widespread devastation and severe flooding in Bangladesh and other countries in the region. The organisation was able to distribute cash ahead of the cyclone because they knew that it was coming. These kinds of approaches of using early warnings to implement early actions will become more and more important in a changing climate. “How can we make use of the available science to be smarter in how we respond?” asked Kelly.

A LOCAL LEVEL RESPONSE BASED ON MULTI-AGENCY PARTICIPATION AND INTEGRATED SOLUTIONS

Cities, more so than national governments, are at the forefront of the consequences of climate change and security threats. If resilience at a local level is to work, we need to break silos in budgeting and mandates. Multi-agency working and practice should be the new order of the day focused on ensuring that communities can bounce back from crises, whether related to climate or security. A “holistic approach and a systemic vision of local development” is needed said Sébastien Maire, Chief Resilience Officer of Paris. “If we look at climate change without taking air quality into account, we will make the same mistakes as before.” According to Maire, the two main challenges in cities now are climate change and social inequality. “The resilience approach is proposing to define solutions that address both at the same time.”

“If we look at climate change without taking air quality into account, we will make the same mistakes as before”

Sébastien Maire
Chief Resilience Officer of Paris

Yet in France, barriers to an efficient holistic approach to local resilience exist in the city administration, which is “more political than administrative” explained Maire. “In all the 25 resilience challenges we identified in Paris, we discovered that the key is governance. It is not technical solutions. It’s how we are going to onboard everyone to reach the solution we’ve been working on.” Within his position, Maire significantly improved territorial governance by helping seven city departments to work together, including those responsible for water, energy, greening and social affairs.

His position is one encouraged by the 100 Resilient Cities, a network that helps cities build resilience to economic, social and environmental challenges. City governance involves an array of distinct actors ranging from government agencies to local businesses, who often don’t communicate well with one another. Moreover, individual cities regularly solve problems already addressed in other cities, which could help them learn from each other.

ROLE OF THE MILITARY

The impact of climate change and security related issues amplify resource competition and increase the risk of instability and violent conflict. Military forces are increasingly preparing for and involved in the consequences. NATO’s 2010 Strategic Concept highlighted that “environmental and resource constraints, including health risks, climate change, water scarcity and increasing energy needs will further shape the future security environment in areas of concern to NATO”. These constraints also have the potential to significantly affect NATO’s planning and operations.

"Climate change is a threat multiplier, it makes other problems worse. It transforms the environment in which the military has to operate. The military is not in the prevention business," he said. "It is basically in the adaptation business"

Michael Ruehle
Head of Energy Security at the NATO's Emerging Security Challenges Division

"Climate change is a threat multiplier," said Michael Ruehle, Head of Energy Security at the NATO's Emerging Security Challenges Division. "It makes other problems worse. It transforms the environment in which the military has to operate." One reason the military is directly concerned with climate change is that it is often the first actor deployed in situations where people are in need. "The military is often the first responder in humanitarian relief situations, whether these are climate change-induced or for other reasons," Ruehle said. "They are there, and the military has to deal with it." However, the role of the military will be different from those of cities and NGOs. "The military is not in the prevention business," he said. "It is basically in the adaptation business."

NATO is doing more analysis on the future security environment, and climate change will play a greater role in this. "We are in the business of looking at energy efficiency standards," said Ruehle. "The military can at least look at technologies that, while maintaining the priority of being militarily effective, are less of a burden on the environment. Military activities are a burden on the environment and there are ways to minimise that ecological footprint."

Climate change, while a global phenomenon, affects different countries at different times and with different intensities. "This means that a nation that doesn't see climate change as an immediate problem will probably focus less on it and its army will focus less on it. There is a general reluctance by countries to engage in discussions that inevitably lead them back to their own national climate policies. You don't want to discuss the linkage between coal and the climate goals, for example. There is a natural reluctance in many institutions – not just NATO – to go too far in a direction that reflects badly on individual countries."

friends of europe

friends of europe

WHY THE CLIMATE-SECURITY NEXUS NEEDS A MULTI-LEVEL GOVERNANCE SYSTEM

A contribution by Kanta Kumari Rigaud is Lead Environmental Specialist at the World Bank Group

As the effects of climate change grow more and more apparent, it has become increasingly clear that climate resilience is now an urgent priority, with the relentless procession of environmentally-wrought catastrophes serving as momentum for the swift employment of mitigation efforts.

In the context of migration, fostering resilience requires not only responding to the displacements caused by extreme weather events, but also anticipating how the consequences of climate change will be made manifest over the coming decades. Even if mitigation efforts are stepped up, it is imperative that there be an increase in the number of multi-level governance structures so as to ensure that the challenges presented by the climate-security nexus are met.

Climate change is a potent driver of internal migration. The World Bank flagship, Groundswell: Preparing for Internal Climate Migration, estimates that by 2050, the impact of slow onset climate change could add more than 143 million internal climate migrants to three already climate vulnerable regions: Sub-Saharan Africa, South Asia and Latin America. Beyond the magnitude of this migration statistic, these numbers are expected to rise even further across all three regions between now and 2050. These trends, which also predict the emergence of spatially concentrated “hotspots” of internal and external migration, will have significant developmental implications. Increasingly, people will move away from those areas that have low water availability, crop productivity and are vulnerable to rising sea levels and storm surges by moving instead to areas that are relatively more attractive in terms of livelihood options. For example, both the delta areas of Bangladesh and the rainfed highlands of Ethiopia have been singled out as hotspots for external climate migration, while peri-urban areas in Mexico’s central plateau are seen as areas that present significant opportunity for future settlement.

While the study indicates that inclusive development and climate friendly pathways could go a long way towards reducing the scale of climate migration – by up to 80% in most cases – the window of opportunity is narrowing fast, with climate impacts intensifying even earlier than anticipated, as early as 2030, if warming is not contained within the 2°C limit.

The expected increase in the pace, scale, and spread of climate migrants as a result of environmental demands early and urgent action from all actors: local, national and global. There is a strong realisation that development frameworks should accommodate migration in each phase of its life cycle (before, during, and after mobility). To date, the work done on addressing climate-induced migration, in addition to mainstreaming these forms of mobility into the larger development context, has been insufficient. Instead, much of the attention has, rightfully so, focused on addressing displacement and crises as driven by natural hazards and conflicts.

Ignoring the reality that climate is a leading driver of migration is no longer an option. To frame the course of action when addressing climate migration, there are two overarching dimensions:

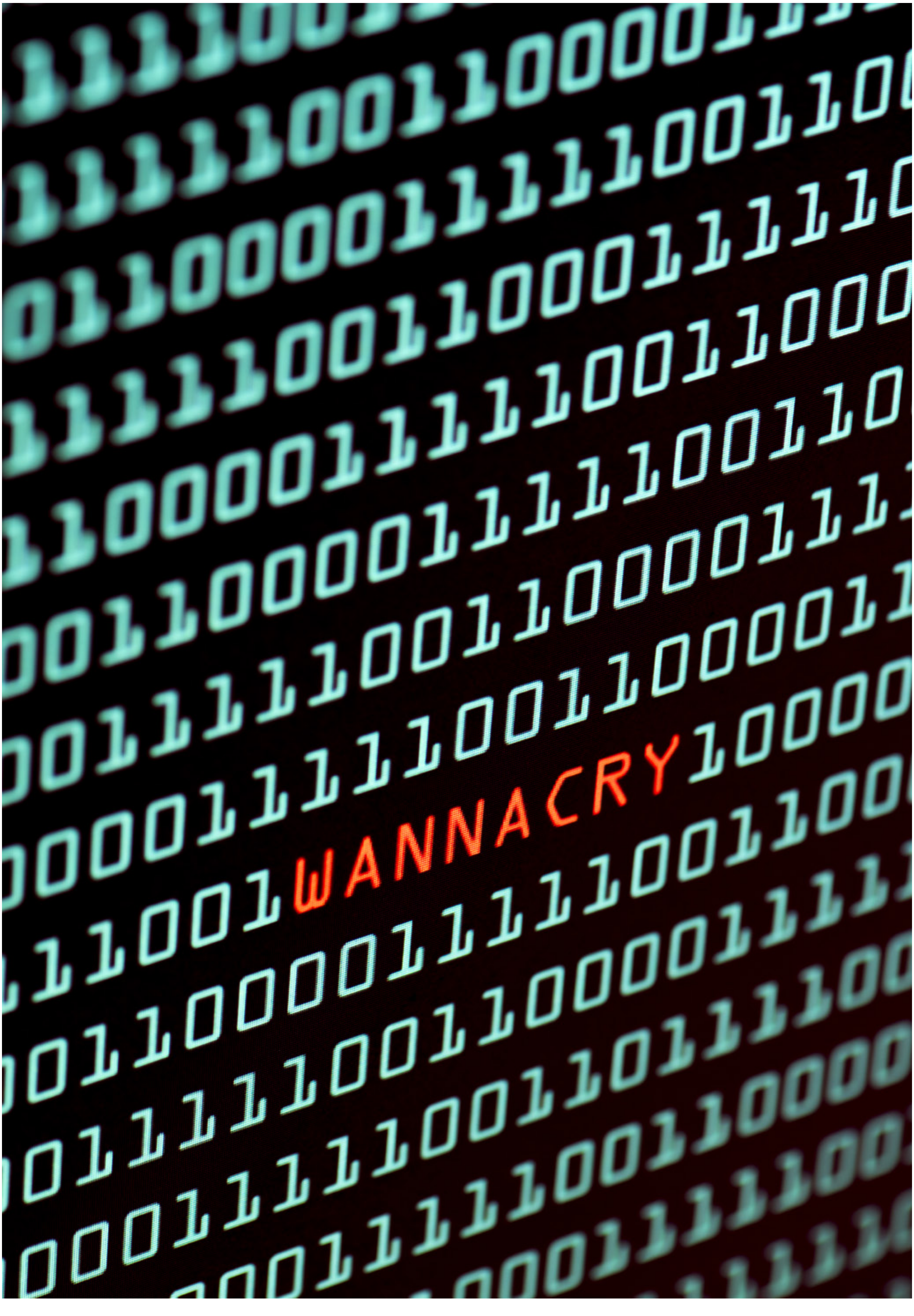
Firstly, targeted investment is needed to better contextualise climate migration, using the best data and models while examining the concerns of decision-makers from the most vulnerable communities in question. Evidence-based knowledge over spatial and multi-decadal time frames is a prerequisite for policymakers to understand, prepare, and address the challenge of climate induced migration in measured and impactful ways, as limited understanding ultimately results in fragmented courses of action. For example, any attempt to understand climate migration patterns in Ethiopia take into account among other factors, the inherent uncertainty of climate models in the region, the most realistic greenhouse gas emissions pathway based on collective global action and the national, and local, trajectory of its development pathway.

Secondly, climate migration demands development policies that anticipate the scale of the issue in the medium to long term. Deliberate action at both global and national levels is an essential way of amplifying attention to climate migration issues over time. The issues are complex and require action from whole continuum of actors: from households and communities who are directly impacted to the global leaders and influencers who are responsible for ramping up mitigation efforts to curtail the intensity of climate change. National actors who drive policy must be aware of these linkages and, as a result, must advocate for the strongest outcomes.

These two dimensions must be reinforced by a multi-governance course of action. A collective, global response to reducing greenhouse gas emissions is the first line of defence in changing the trajectory of climate risks and impacts, and consequently of climate-induced migration at community, district and state levels, where most mobility-related decisions are made.

At the same time, strong national policies and frameworks that pursue inclusive climate-smart policies will assure transformational outcomes. Incremental, low-regret measures alone may not be enough to counter the scale of impending climate migration. This is particularly the case for low-income countries with high population growth, such as Ethiopia, where the bulk of the population is engaged in agriculture, rainfed, areas that are particularly climate sensitive. An economic transition towards sectors that are less sensitive to climate change also needs to be part of the long-term solution. Meanwhile, targeted interventions can also be deployed in the short- and medium-term to support migrants at community levels. Good practices, including facilitating informed decisions on migration, making social protection portable and scalable and tapping the potential of financial and social remittances will be central to the strategy. Remittances continue to be an important strategy in Bangladesh, Mexico and Ethiopia, countries of special focus in the Groundswell report.

Multi-level governance is an imperative for delivering sustainable, durable solutions for the human-climate security nexus. Climate migration is a reality, but it does not have to be a crisis.


WANNACRY

PART 3 | BUILDING CYBER RESILIENCE
ALIGNING STRATEGIES AND INCREASING COOPERATION

INTRODUCTION

Europe's latest cyber defence plans and projects are reason for cautious optimism, according to a panel of cyber experts gathered in Brussels on 6 November 2018 for 'Building cyber resilience: aligning strategies and increasing cooperation', the third Friends of Europe debate on resilience. "The empire seems to be striking back, thanks to the EU's playbook of responsive measures to improve resilience, deterrence and to hold cyber-attackers to account," said Jamie Shea, Senior Fellow at Friends of Europe.

"The empire seems to be striking back, thanks to the EU's playbook of responsive measures to improve resilience, deterrence and to hold cyber-attackers to account"

Jamie Shea
Senior Fellow at
Friends of Europe

Disruptive and malicious cyberattacks increasingly threaten our lives and society at every level. They cost the world €235 billion in 2017, with the NotPetya attack alone racking up corporate losses in the hundreds of millions. The WannaCry ransomware attack perpetrated by North Korea infected 300,000 computers across 150 countries and brought chaos to the United Kingdom's National Health Service hospitals. Deterrence and resilience are key to being able to withstand, recover and respond to these malicious assaults.

Building on the 2016 Warsaw Joint Declaration, the European Union and NATO have stepped up their cybersecurity measures and capabilities. These include extended partnership – such as coordinated exercises ranging from prevention, crisis management and recovery – and even the prospect of striking back at cyber foes. Yet, is the EU-NATO cooperation mature enough to enable both organisations to make a comprehensive contribution to cybersecurity? And are current international norms enough to govern conduct in cyberspace? There is also concern about Europe's ability to secure its cyber domain, given the new threats emerging alongside technologies like 5G and artificial intelligence (AI).

STEPPING UP EUROPE'S CYBER RESPONSE

In 2016, NATO signed a Technical Arrangement on cyber defence cooperation with the EU, while NATO Allies made a Cyber Defence Pledge to enhance their cyber defences. The EU boasts an ever-expanding playbook of cyber defence measures, such as the €13 billion European Defence Fund, EU Cyber Rapid Response Force teams and Permanent Structured Cooperation (PESCO) on security and defence. There is also new EU-wide legislation on cybersecurity, centred round the 2016 NIS Directive on the security of network and information systems.

“Cybersecurity is a cross-border issue. Estonia is more resilient today, thanks to better coordination and international policies on cybersecurity, especially at EU and NATO levels”

Heli Tiirmaa-Klaar
Estonian Ambassador for Cyber Security

“The focus is on better preparation for cyberattacks through exchange of information, underpinned by the NIS Directive”

Vivian Loonela
Member of Cabinet of Andrus Ansip, Vice-President for the Digital Single Market at the European Commission

Over the last year, the EU and NATO have also enhanced cooperation to ensure complementarity of measures, under the EU Joint Framework on countering hybrid threats. This framework aims to improve situational awareness, resilience of critical infrastructure (e.g. transport, communications, health services, energy, banking and finance) and responses from the EU and member states.

Cyberattacks on Estonia in 2007 were a huge wake-up call for Europe. Is the country better prepared for them today? “Cybersecurity is a cross-border issue. Estonia is more resilient today, thanks to better coordination and international policies on cybersecurity, especially at EU and NATO levels,” replied Heli Tiirmaa-Klaar, Estonian Ambassador for Cyber Security. For example, the country’s maritime sector escaped the tsunami-like damage of a cyberattack that recently hit a quarter of the world’s shipping and ports industry.

KEYBOARD CYBERWARRIORS

Estonia can also rely on the skills of its Defence League’s Cyber Unit, whose volunteer specialists (including many IT professionals) protect national cyberspace, in cooperation with the government. The UK, France and the Netherlands too now have ‘cybercitizen armies’, complementary to military initiatives and cyber defence agencies springing up across Europe.

Where then does Europe stand on cybersecurity today? “The focus is on better preparation for cyberattacks through exchange of information, underpinned by the NIS Directive,” said Vivian Loonela, Member of Cabinet of Andrus Ansip, Vice-President for the Digital Single Market at the European Commission. She also highlighted a push for better hardware and software, with a proposal for substantial cybersecurity investments in the next EU budget. “Cyber hygiene is also important, because we’re all responsible for securing our computers and networks,” remarked Loonela. She noted a growing public awareness of cyber risks, reflected in the fact that cyber features on the agenda of every European Council meeting.

The EU is doing everything it can to boost cybersecurity, and that includes driving the Digital Agenda, said Loonela. “There are two million IT jobs going unfilled in Europe, due to the difficulty of finding people with appropriate skills,” she noted. “We need more digital education and training, which will also empower our citizens to fend off cyber threats at every level.” NATO is improving its cyber education and training and the skill sets of its operators, including through the setting up of a cyber academy at the CIS School, remarked Sorin Ducaru, Chairman of the NATO Secretary-General’s Senior Advisory Board for the Functional Review of the NATO Headquarters, Special Advisor at the Global Commission on the Stability of Cyberspace, and Trustee of Friends of Europe.

Asked how NATO's Cyber Defence Pledge helps the Alliance's members, Ducaru picked out three advantages. Firstly, the pledge has got European leaders talking about cybersecurity and put it at the centre stage of politics. It has also set some related standards beyond military infrastructure. Lastly, it has led to cyber defence capability development and better institutional frameworks in NATO countries. Even better, a 2018 review indicated the pledge is stimulating inter-government and inter-agency work and cooperation on cyber defence.

"NATO has declared cyber as an operational domain, keeping the resilience focus while understanding that the Alliance must now take a broader approach," said Sorin Ducaru. Practically speaking, that means a "mission assurance paradigm", where it is accepted that a cyberattack will degrade some systems. However, thanks to systems redundancy and other capabilities, it should still be possible for NATO members to complete their mission goals. "So NATO may employ offensive capabilities, but always within international law through a defensive mandate, its major objective for the last seven decades," he added.

Ducaru said that NATO is now considering "imposing costs" for a cyberattack that hits a member country: "NATO links cyber defence to its core business, so could respond when cyberattacks reach the threshold of armed attacks or if they have the same implications as conventional attacks, in accordance with Article 5 on collective self-defence." On the EU side, several countries named and shamed Russia for its state-hacking activities: "It remains to be seen if this measure, or using attribution and economic sanctions, will assist our bloc's cyber defence," said Vivian Loonela, from the European Commission.

After noting his support of EU-NATO cooperation, with cyber at the forefront, Ducaru welcomed the EU's "cyber diplomacy toolbox" – a range of diplomatic, political and economic assets that could be wielded to retaliate against a cyberattack on the bloc. Among other technical and political measures, NATO and the EU are developing cybersecurity rapid response teams for mitigation, forensics, and sharing information.

BOLSTERING THE CONTRIBUTION OF BUSINESSES

The private sector is eager to play a larger role in cybersecurity. Ruth Davis, Head of Commercial Strategy and Public Policy at BT Security, said: "As a provider of the UK's critical national telecoms infrastructure, we focus on securing our networks because security is integral to our business." However, the company is also ready to share information on cyberattacks with its competitors and intelligence agencies. For instance, it can pin down ("attribute") the source of any cyberattacks by scanning BT's global networks.

> **"There are two million IT jobs going unfilled in Europe, due to the difficulty of finding people with appropriate skills. We need more digital education and training, which will also empower our citizens to fend off cyber threats at every level"**
>
> **Vivian Loonela**
> Member of Cabinet of Andrus Ansip, Vice-President for the Digital Single Market at the European Commission

> **"NATO has declared cyber as an operational domain, keeping the resilience focus while understanding that the Alliance must now take a broader approach"**
>
> **Sorin Ducaru**
> Chairman of the NATO Secretary-General's Senior Advisory Board for the Functional Review of the NATO Headquarters, Special Advisor at the Global Commission on the Stability of Cyberspace and Trustee of Friends of Europe

“We must also create a market for secure-by-design and educate consumers about the importance of secure devices and mobile apps, possibly through a new labelling system”

Ruth Davis
Head of Commercial Strategy and Public Policy at BT Security

“There is no uniform approach to cybersecurity across the private sector,” added Davis. She noted how BT ensures all its products undergo a full security review before getting their “security passport”. The UK government has also launched voluntary secure-by-design guidance for Internet of Things (IoT) manufacturers. But if product certification like this is to be effective, it may have to become mandatory. “We must also create a market for secure-by-design and educate consumers about the importance of secure devices and mobile apps, possibly through a new labelling system,” said Davis.

There are both opportunities and challenges about the possible impact of next-generation 5G telecoms networks, AI and cloud computing: “These sophisticated technologies can be vectors for further cyberattacks, yet they also promise more resilient networking and cyber solutions such as stronger encryption.”

CYBER DEFENCE: WHAT ELSE IS IN THE TOOLKIT?

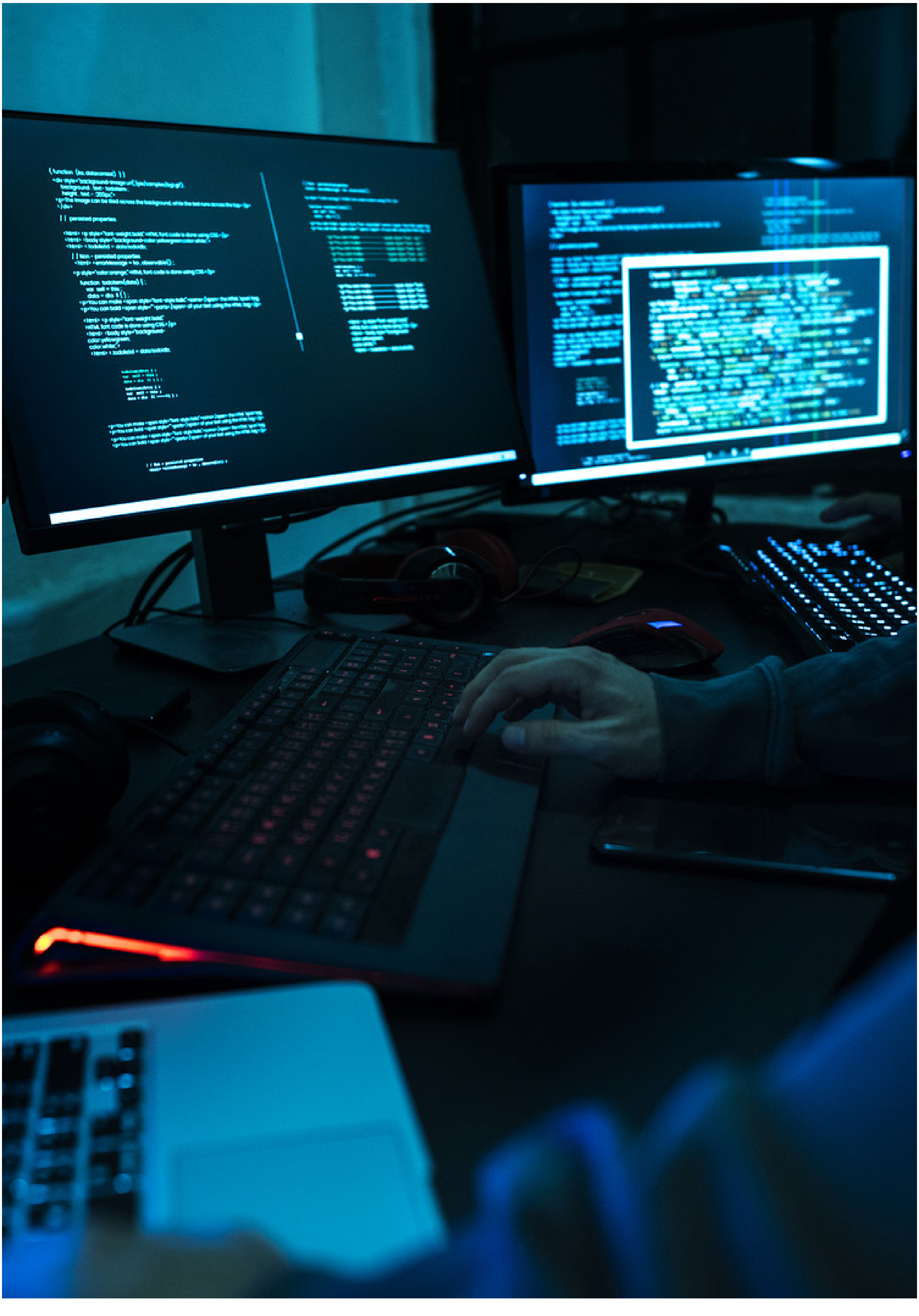
While investing in cyber defence is a major economic cost for governments, this can be addressed through more public-private partnerships as well as further NATO and EU investments. Other solutions for cyber defence could include safer software, security throughout supply chains and active cyber defence by strengthening web infrastructure and protocols. There was consensus too on the value of the EU General Data Protection Regulation (GDPR), which has focused people’s minds on security, privacy and data ownership in Europe and beyond.

“International law applies to cyberspace, though we don’t yet know how exactly. The UN and many governments are slowly developing norms on cyber behaviour, which we can then build on,” said Heli Tiirmaa-Klaar, Estonian Ambassador for Cyber Security. “We need to work on all aspects of cybersecurity, since there is no silver bullet on the horizon,” concluded Jamie Shea. He underlined the inevitability of serious cyberattacks in the future. However, thanks to growing awareness of this risk, NATO and the EU are coming together more in the virtual space and further developing their counter-measure responses.

friends of europe

friends of europe
Connect. Debate. Change.

friends of europe
5 NOVEMBER 2018
BUILDING CYBER RESILIE
ALIGNING STRATEGIES AND IN
COOPE



WE NEED TO OVERCOME TRUST ISSUES IN CYBER SECURITY - BEST PRACTICES FROM LITHUANIA

A contribution by Edvinas Kerza is Lithuanian Vice-Minister of Defence

It is no wonder that with such attributes as the ease of launching an attack, the ability to hit multiple sectors or countries at once and the difficulty to identify the perpetrators, cyber threats thrive in today's hybrid environment.

The ever-increasing digitalisation of everyday activities makes the cyber domain both a safe haven for malicious actors and a headache for governments and companies that are trying to protect themselves against the increasing threats and attacks. In the case of Lithuania, for example, the Lithuanian National Cyber Security Status Report 2017, conducted by the National Cyber Security Centre (the NCSC) under the Ministry of National Defence (the MoND) of the Republic of Lithuania, reveals that when it comes to cyber attacks, the most targeted sectors in the country are energy, public security and foreign affairs. One can easily see how vulnerabilities in these sectors could lead to consequences that are severely damaging, such as disturbance of energy supply, compromised police work and the loss of classified information.

An equally disastrous ripple effect is caused if social engineering tools are employed in operations ranging from financial extortion to stealing official government data. Or, in a true hybrid fashion, attacks may combine both cyber and information elements. Earlier this year, a Lithuanian news website was hacked to post fake messages about Lithuania's defence minister, simultaneously sending e-mails with infected links to numerous recipients. The hacker's IP address was traced to Russia.

Lithuania's cyber security system, which has already undergone its growing pains, could be taken as a positive example

Against this backdrop of cross-sectoral and cross-border effects of cyber threats, the most logical response is an integrated public-private cyber security system at the national level, complemented by a high degree of international cooperation. While it might not be easy to achieve, it is surely not impossible.

Lithuania's cyber security system, which has already undergone its growing pains, could be taken as a positive example. In 2015, the Law on Cyber Security was passed, distributing various responsibilities among national institutions. Soon enough, it became apparent that there were still obvious functional overlaps and inefficient distribution of resources. At the same time, governmental and business entities found it difficult to address the right institution in case of an emergency. This led to the decision to consolidate all cyber responsibilities under the the MoND and the NCSC, thus creating a single authority on cyber security for both public and private entities.

A crucial element in implementing these reforms was the issue of trust-building. It started within the National Defence System with the aim of creating synergy between the MoND and the Armed Forces, so that both institutions would see themselves as integral parts in dealing with cyber issues. The next step was to engage other public and private actors, encouraging them to open up their networks, share information and internalise the responsibility to fulfil organisational and technical cyber requirements. A number of practices have been set up to contribute to trust-building: annual public report on cyber security to raise the general awareness and understanding of cyber threats; regular state-wide cyber exercises and other educational activities for developing practical skills and working relations among various entities; cooperation with the media, and so on.

The issue of trust becomes even more prominent at the international level. While governments can introduce various forms of penalties for failing to comply with cyber regulations nationally, most international organisations lack this type of authority. Therefore, one cannot highlight enough the unique role that the European Union plays in this area. Through its legislative powers, the EU can set unified standards not only for public, but also for private entities, as shown by the recently adopted legal acts the General Data Protection Regulation (GDPR) and the Directive on Security of Network and Information Systems (the NIS Directive). Of course, it often falls to the EU member states to implement the law and for public and private companies to adhere to its provisions. This circles back to the individual states and the efforts they put into building robust national cyber security systems.

Cyber is proving to be the area where the EU can create value-added without duplicating NATO's efforts

An even bigger qualitative leap is being made in the EU within the PESCO framework with the project "Cyber Rapid Response Teams (CRRTs) and Mutual Assistance in Cyber Security". The initiative, proposed and led by Lithuania, foresees that member states do not only share information and expertise, but also pool human resources to handle and deal with cyber threats. The CRRTs will assist the participating nations in case of cyber attacks and could even be deployed in support of the EU institutions or operational activities.

From the inter-institutional perspective, cyber is proving to be the area where the EU can create value-added without duplicating NATO's efforts. Therefore, it is necessary to further facilitate information exchange and improve communication channels between the two organisations. At the same time, it is important to expand the network of like-minded countries and share best practices with NATO and EU partners. Lithuania has been successfully doing this with Ukraine and Georgia.

As cyber threats become more complex, individual states and international communities cannot afford the luxury of lagging behind in terms of strategies, methods and tools. In Lithuania's experience, a single ownership of cyber security authority, together with consistent communication, helps to develop trust and bring different actors and stakeholders together.

Yet, national efforts are not enough. The transnational nature of cyber threats can only be adequately addressed if there is readiness to engage in a conversation and action. The EU has the instruments to spur a more vigorous move in this direction where states are willing to share their knowledge and capabilities for the sake of common security and tangible results. However, the key takeaway is that practice makes perfect: fostering trust must be regarded as a continuous investment, especially when progressing from national solutions to ambitious international initiatives.

CONCLUSION

Our societies are deeply interconnected: as a result, any vulnerabilities in infrastructure have wider societal implications. Can we still talk about creating security or should achieving resilience become our primary goal? In this report, we argue that today's threats come in a variety of different forms, causing severe damage to governments, private companies and individuals alike.

Transnational threats like climate change contribute to a sense of helplessness when it comes to confronting the challenges that face us. Cyberattacks demonstrate that without effective cooperation between private and public sectors, civil awareness and vigilance, anyone can be vulnerable. Recent acts of terrorism have resulted in a reassessment of the ways in which we think about urban design. Attacks that consist of multiple elements exploit vulnerabilities and cause grave ripple effects. Do we need to fundamentally rethink the purpose and structure of our defence and security capabilities?

Security-by-design entails discovering and reconsidering potential vulnerabilities in order to avert their abuse. Novel approaches, such as the avocado-model in cyber security, entail a rethinking of the design and purpose of the tools we have at hand when securing data. The traditional coconut-model in cyber security functions as a hard 'shell' that protects the important data held within. However, with this method, it is often difficult to identify security breaches before critical data has been stolen or infected. The avocado-model, on the other hand, encrypts the most valuable data in a safe core, with a layer of non-sensitive data the first accessed when an entry is broken, surrounding it. This method allows more time for cyberattacks to be counteracted before serious harm is inflicted.

In cities, fostering resilience and making urban life secure means re-thinking open spaces and city infrastructure to prevent soft-target attacks. The full range of agencies involved in urban crisis-management must therefore practice scenarios to collectively understand the chains of command and responsibilities in the event of a crisis. Taking a more strategic and holistic approach to threats caused by climate change can prevent climate change from becoming the threat multiplier that it is today.

Coordination between the local agencies directly affected by crisis situations needs to be complemented by international cooperation and information sharing. Cities already share their best practices with each other. Improved coordination on international policies has meant that cyberspace has become a more secure place at both NATO and EU levels. Reaching resilience requires clear structures, joint efforts and a fundamental rethinking of our infrastructure, its purpose and design. Resilience is best built together.

In a time when all vulnerabilities cannot be pre-empted, building resilience is our best bet.

Friends of Europe
Connect. Debate. Change.

+32 2 300 29 92
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.