
debating+ security
friends of europe
Debating Security Plus 2019
REPORT

Debating Security Plus (DS+) is a global online brainstorm, bringing together over a thousand participants from 86 countries, with the aim of crowdsourcing policy recommendations to the world's security threats. The brainstorm spans international security architectures, cybersecurity defence and deterrence, urban management, arms control and disarmament, EU-NATO's defence capabilities in Europe's eastern and southern neighbourhoods, migration and human security, and transatlantic relations. DS+ is part of Friends of Europe's Peace, Security and Defence programme, and supported by the United States European Command (EUCOM).

Unless otherwise indicated, this report reflects the rapporteur's understanding of the views expressed by participants. These views are not necessarily those of the partner organisations, nor of Friends of Europe, its Board of Trustees, members or partners.

With the support of

Civocracy

Co-funded by the Europe for Citizens Programme of the European Union

In partnership with

Clingendael
Netherlands Institute of International Relations

INDEPENDENT DIPLOMAT
The Diplomatic Advisory Group

EUROMIL

Editor: Geert Cami
Publication Director: Nathalie Furrer
Programme Managers: Elena Saenz Feehan, Antonia Erlandsson
Programme Assistants: Gerard Huerta, Katherine Pye
Editor: Arnaud Bodet
Designer: Lucien Leyh

Table of contents

Introduction

Friends of Europe's unique global online brainstorm, Debating Security Plus (DS+), is the only virtual meeting forum that permits a truly global whole-of-society consultation and gathers a broad range of ideas to discuss some of the world's most pressing security challenges.

For its seventh edition in 2019, Jamie Shea, Senior Fellow at Friends of Europe and former NATO deputy assistant secretary-general, gathered an exclusive community of hand-picked experts knowledgeable on peace, security and defence who were regularly consulted via online. Our DS+ debates were held entirely online and our experts took part in them from all around the world from their computers or smart phones.

By actively engaging and sharing their expertise in a global debate, our community of seasoned experts and practitioners ensured the highest level of dialogue, helped to formulate concrete and in-depth solutions, facilitated new networks, and proposed options for decision-makers. Outcomes from previous security brainstorms that Friends of Europe has organised have informed the implementation of the EU Global Strategy, as well as the policies of national governments and other international institutions as they shape their approaches to peace, security and defence.

Throughout the year we offered exclusive webinars, live debates and flash-reactions to security-related events with our community on our platform so that they could engage and provide their expertise. This report gathers our community of expert's thinking and ideas on topics such as:

- The climate-security nexus
- Women in security
- Next level disinformation: deep fakes
- Space: the next frontier?
- Nuclear proliferation and non-state actors
- AI in defence: what would an AI code of conduct look like?
- Hybrid warfare and biological agents: bio-threats and bio-terrorism
- Internet governance and cyber security

We hope that this report will be of interest to you and a source of ideas an inspiration for your own work in these fields.

Resource scarcity and conflicts

Water availability and the climate-security nexus

Introduction

The new year had hardly begun when we were confronted with more frequent and more dramatic news about the accelerating impact of climate change on our planet. The American Midwest was in the grip of a polar vortex with incredibly low temperatures and schools and offices closed while in Australia temperatures were above 40°C and the country was in the midst of a prolonged drought. Subsequently this led to the worst bush fires in the country's history, with the other 14mn square kilometres of territory devastated and half a billion animals killed.

The last three years globally have been among the hottest on record. The polar ice pack is melting at four times the previously estimated rate and the Antarctic, long thought to be more stable, is now showing signs of stress as well. More than 75% of the earth's land is now seriously downgraded and 30% of the arable land has been lost over the past seventy years.

As climate change accelerates, we are becoming more aware of its impact on human security. Migration, water and food scarcity and rivalries over control of key resources could be the main drivers of conflict and international competition in the 21st century. Yet the mounting urgency of reports and scientific analysis is not yet matched by the attention climate change and resource scarcity are receiving in the politics of the world's major powers.

On the other hand, intelligence agencies and the military are increasingly factoring in climate-driven scenarios into their forecasting and planning, as these could put many of the world's poorer and more fragile countries under extreme social stress, rapidly exporting their instabilities to their neighbours and beyond. Understanding how aspects of climate change and social breakdown and conflict impact on each other in a mutually reinforcing loop is urgent for all security practitioners.

Why is it that the politics of climate change are not keeping up with the mounting scientific evidence about its impact? How can we persuade our politicians to act and to implement their promises to take action more vigorously? Which scenarios in terms of resource scarcity and potential conflicts should we have on our watch list? Will we start seeing water wars in the near future or conflicts over arable land or grazing rights? What does climate change mean in terms of our current foreign and security policies? Are our military forces ready and equipped to respond to climate-induced crises and conflicts? Are we doing enough to help the vulnerable countries with adaptation, mitigation and resilience strategies?

Our discussion on the climate-security nexus brought many interesting insights from across the globe. The Debating Security Plus team also joined the annual Planetary Security Conference organised by the Foreign Ministry of the Netherlands and the Clingendael Institute in the Hague.

What do the experts think?

As **Leona Romeo-Marlin**, Prime Minister of St Martin, argued¸ climate change causes natural disasters with devastating economic, financial and social consequences that directly affect peace and security. “The world is interconnected; what happens in our region will affect yours. Global interaction, global cooperation and global action is therefore required.”

Celine Charveriat, Executive Director at the Institute for European Environmental Policy (IEEP), explained that in the period from 1970 to 2017, the global extraction of materials increased by more than 240%. Resource scarcity is an environmental driver commonly linked to conflicts around the world and the way companies and citizens extract and consume these resources has a direct impact on climate change and global security. This is why, according to Charveriat, we need to move to a more circular economy, reducing the use of resources substantially.

Monica Sanders, Lecturer at Georgetown University, argued that to achieve this shift, we need to find ways to understand what the cost of adaption is across groups and figure out ways to make these changes acceptable. “The issue here is not how to persuade politicians to change. It is about offering them a manageable pathway to change”.

These changes should also apply to the military forces as they are both causing and

"The world is interconnected; what happens in our region will affect yours. Global interaction, global cooperation and global action is therefore required"

Leona Romeo-Marlin, Prime Minister of St Martin

suffering the consequences of climate change. **General Tom Middendorp**, Chief of Defence of the Armed forces of the Netherlands until 2017, who we linked up with in The Hague, stated that looking at only military threats is no longer valid. “Climate and security are both topics that are of existential importance to anybody”. Therefore, the military needs to prepare to address expanding threats provoked by climate change in all their missions and no matter where they are while also being part of a wider solution to these threats. To do so, a whole of government approach is necessary.

US Navy **Rear Admiral Ann C. Phillips** at the same meeting, argued that the military should continue developing new technologies and strengthen the relationship between the military, research, and development to facilitate military missions and increase resilience to climate change.

Sherri Goodman, Senior Advisor for International Security at The Center for Climate and Security, added that legislators should hold agencies to account on how they carry out the adaptation and deal with climate change: “the opportunity, and challenge, is still connecting the dots between climate and security”.

Women in security

Introduction

It hardly needs to be said that as women represent 50% of the global population, the success of any individual country, business or human enterprise depends on the ability to integrate women and give them full opportunity to use their skills and talents. As a whole series of Arab Development Reports issued by the United Nations in recent years have underlined, failure to achieve this goal puts a severe brake on economic development, technological progress and the creation of jobs and skill sets. It is not simply a matter of justice and human rights but also of economic growth and social mobility.

Certainly, at the top political level, the role of women in peace and security as well as their protection and wellbeing in conflict zones have received attention. UN Security Council Resolution 1325 – on the unique impact of armed conflict on women and girl – was adopted as far back as October 2000. NATO has now its third Special Representative of the Secretary-General for Women, Peace and Security. It has adopted measures against trafficking and to incorporate gender advisers into its military stabilisation and training missions in Afghanistan. Meanwhile the globally networked organisation, Women in International Security, continues to nurture future female talent as well as produce women leaders in the field, including NATO's first female Deputy Secretary-General, Rose Gottemoeller. Friends of Europe has supported this effort as well.

Yet if there has been progress, there is still a massive amount to be done. Some notable success stories of women leading in diplomatic, military or advocacy roles does not mean that women are achieving equality or full participation in every domain of today's crowded and taxing security agenda.

If there are obstacles where are they and why? Is it leadership at the top or bureaucratic inertia lower down? We also want to look at the success stories. Where and how are women making a real difference to peace and security? How are women protecting other, more vulnerable women? Which countries and organisations are performing the best and which lessons and guidance can be transmitted to others so that they do not repeat the same mistakes? Where there are gaps, what do we need to do to remedy them and are our existing policies and instruments up to the job? How can the tasks involved in peace, security and defence be made more attractive to potential women candidates and how can we develop the appropriate career structures to encourage more top-quality women to step forward?

Coinciding with International Women's Day, Friends of Europe launched a discussion on women in security to spark a conversation on the global effort towards the empowerment of women in achieving security and gender equality.

In partnership with Independent Diplomat, a non-profit organisation that advises governments and democratic groups across the world, we met with women from southern Yemen to talk about their involvement in the peace process.

What do the experts think?

When talking about post-conflict reconstruction, **Alice Musabende**, Gates Scholar in Politics and International Studies at Cambridge University, stated that women need to be part and parcel of all the institutions involved in the process. She explained that the Rwandan transition was a success because it institutionalised the contribution of women to peace and decision making.

On that note, **David Fouquet**, President of the European Institute for Asian Studies, argued that it is important to look beyond our Eurocentric perspective and learn from other societies, such as Ethiopia and Rwanda. Both countries have successfully recognised the role of women in governance and have given women and peace a chance.

Monica Sanders, Professor and Policy Director at Georgetown University, stated that EU reforms should not only focus on gender diversity but also on ethnic or cultural diversity, as they would better represent the population of member states.

The European Organisation of Military Associations (EUROMIL) also advocated for more diverse and inclusive armed forces arguing that they better reflect the societies they serve, they are more effective at fulfilling their tasks and they create a better working environment for all employees.

Clare Hutchinson, NATO Special

"Women are not merely victims of conflict but also play active roles as combatants, peacebuilders, politicians and activists, and are often in the strongest position to bring about peace in their communities"

Clare Hutchinson, NATO Special Representative for Women, Peace and Security

Representative for Women, Peace and Security, explained "women are not merely victims of conflict but also play active roles as combatants, peacebuilders, politicians and activists, and are often in the strongest position to bring about peace in their communities." This is why it is imperative to integrate a gender perspective into the multidimensional comprehensive approach required to fight the symptoms and address today's security threats.

Rory Keane, Head of the United Nations Liaison Office for Peace and Security in Brussels (UNLOPS), argued that the inclusion of women in peace operations is essential because they increase their effectiveness – as operations are more legitimate because they reflect society and give a sense of confidence to people on the ground – and they produce a more sustainable peace in the long term.

Kyra Luchtenberg, Policy Officer at Independent Diplomat, explained that women participating in peace negotiations are more likely to adopt collaborative approaches and organise across ethno-sectarian divisions than their male counterparts. Therefore, adopting token gender quotas is not enough. Women's effective and meaningful participation should be enabled. Moreover, gender vulnerabilities are often linked to the root causes of the conflict, so gender perspectives should not be strictly limited to 'gender issues.' On the contrary, they need to be incorporated across all issues addressed at the negotiating table.

On the same page, **Fernando Aguiar**, Genderforce, Gender and Security Analyst/ BICRHR, Manager of Research and Strategic Adviser on Conflict and Security, argued that "instead of focusing solely on numbers, the international community might do well to think with a broader understanding of gender relations and focus on changing policies as well as structures that perpetuate gender inequalities within and beyond the security sector".

When talking about the new security challenges that women are facing, **Mara Marinaki**, EEAS Principal Adviser on Gender, explained that cyber Violence Against Women and Girls (VAWG) is affecting more than 10% of women older than 15-years-old globally and that is it essential that cyber VAWG be legislated at the EU level.

Next level disinformation

Deep fakes

Introduction

Propaganda and interference are nothing new. Psychological operations and the fuelling of culture wars have traditionally been part of the repertoire of conflict. States will seek as far as possible to obtain the fruits of war (influence, leverage and advantage) through competition short of fighting and below the threshold where their adversaries would feel compelled to escalate or respond with force.

But what is new is that modern technologies make it easier and cheaper to conduct disinformation campaigns on a semi-permanent and more targeted basis. This allows more players in to get into the game. In polarised societies, prone to populism and ready to believe the worst of their opponents, this disinformation is rapidly disseminated and picked up. A recent study by the Massachusetts Institute of Technology (MIT) has shown that fake news spreads across the Internet at six times the speed of genuine news. It reinforces the breakdown of societies in which truth becomes what people want to believe.

Of late, social media companies such as Facebook or Google have shown more willingness to take responsibility for addressing this problem by hiring more fact checkers and removing more fake news sites, even if the effort is sometimes slow and sporadic. But what if technology is evolving faster than the capacity of social media companies and the regulators in government to control it?

We have already experienced this problem with artificial identities created by bots. Now we have 'deep fakes' which impersonate the images and voices of people, making it increasingly difficult to distinguish reality from fiction. We have seen in the dispute between Saudi Arabia and Qatar how the manipulation of deep fakes can provoke a major diplomatic row between two countries that are key to Middle East security.

So how bad is this problem? How good will the technology be in the future? Can we find effective ways of identifying these deep fakes before a serious crisis results? What are the responsibilities of the social media companies and traditional media? What about the role of the regulator and of the law? Are there best practices in countering deep fakes that we can learn from?

The Debating Security Plus discussion on deep fakes gathered strategic communication and technology experts to address these questions and many more.

What do the experts think?

Speaking about deep fakes, **Clare Moody**, a Member of the European Parliament, cautioned that deep fakes and disinformation will exploit the lack of trust citizens currently have in European governments. She argued that growing distrust could be hugely damaging for Europe's democratic system if no decisive action is taken. "We have to look at it in the same way that we are responding to terrorism videos. These are all fundamental attacks on our fellow citizens, on humans."

Ruben Arcos, from the University Rey Juan Carlos in Madrid, explained that denial and deception have long played an important role in our strategic communications. However, he argued that as new technologies like deep fakes emerge, governments and other actors could easily discredit and mock the opposition or vice-versa, posing a great threat to our liberal democracies. The audio-visual nature of deep fakes could be used with the intent to create an alternative reality in the minds of citizens for different aims.

Within the EU context, **Giles Portman**, from the EEAS East Stratcom, called out Russia for using disinformation campaigns to interfere in recent elections across Europe, warning that these mechanisms are well organised and well-funded. This calls for an attentive and resilient strategy from the EU's side.

Showcasing the malleable nature of fake news, **Tom Law**, from the Ethical Journalism

"We have to look at it in the same way that we are responding to terrorism videos. These are all fundamental attacks on our fellow citizens, on humans"

Clare Moody, Member of the European Parliament

Network, argued for the need to offer guidance to journalists on practicing ethical and objective reporting and avoiding falling into the misinformation trap. This is particularly an issue when it comes to reporting on migration. To ensure accuracy in reporting, knowledge of the law and media frameworks is crucial. **Hany Farid**, from Dartmouth College, warned that we should not take objective journalism for granted. He claimed that the surge in disinformation can, in part, be linked to lower citizen engagement with the news.

Looking towards the responsibilities of 'big tech', Farid added that social media companies already have 'Terms of Use' rules that need to be implemented and that these companies have a responsibility to clean "the mess they have created". This includes revising social media companies' monetising models. Currently, they depend on users spending more time on their platforms, incentivising the platforms to prioritise engagement over meaningful content. Governments should work closely with these companies to make sure that they are "walking the talk".

Shamir Allibhai, from Amber Video, concluded that blockchain brings hope to the challenges posed by the new technology of deep fakes, due to its transparency and potential to track evidence. Blockchain could provide a clearer picture regarding the origin of fake videos, as well as how and when they were altered. This could help prosecutors accurately attribute those responsible for creating malicious fakes and hold them accountable.

Space: the next frontier?

Introduction

Traditionally, competition and conflict among states have taken place on land, at sea and in the air. In recent times we have added cyber as a fourth domain of warfare as the information and digital dimension of operations has become ever more decisive. Yet at the same time, another area of rivalry has opened up which has received much less attention but which is becoming more contested and holds the key as much as the other domains to success in future conflicts. This is space.

Today 58 countries have spaced-based assets, and they are critical for all the vital functions of the global economy and our high-tech societies. Satellites govern weather forecasting, tracking and positioning, the timing of billions of financial transactions, communications and for military forces' precision targeting of weapons systems and early warning of missile launches.

Unsurprisingly, space is drawing more attention from military establishments. Back in 2007, China launched its first anti-satellite missile (ASAT) causing thousands of pieces of space debris to orbit the earth. India followed suit in 2019. Iran and North Korea have both launched satellites showing that the barriers to entry as a new space power are becoming lower all the time. Indeed, most of the satellites to be launched in the next few years will come from the private sector, notably by Elon Musk's SpaceX company. What is clear is that space is becoming ever more congested and contested.

NATO countries currently own 65% of global space assets so the growing dependency on access to space is a new concern for the Alliance's policy planners and strategists. Particularly when we remember that private sector space assets provide 70% of the Allies' communications during operations. In 2018, a Russian satellite manoeuvred perilously close to a French satellite, serving as a timely warning sign. Already President Trump has established a new Space Force and Space Command under the aegis of the US Air Force. Meanwhile, NATO heads of state declared space as an operational domain at the December 2019 London Summit.

The EU is also endeavouring to play an increasingly important role in space through the European Space Agency, the Galileo European global satellite-based navigation system and Ursula von der Leyen Commission's new DG Defence Industry and Space.

Does this mean that future conflicts will be won or lost in space? Should the focus of military planning and capability development shift to that realm? How will space impact on future operations? Are the European and transatlantic allies well positioned to operate and compete in this domain? What are the gaps and vulnerabilities that we need to address? Is this an area where the EU has to follow the US lead or can it play a leading role in its own right? Is the time right to look at arms control in space? Which objectives in particular should

arms control pursue and can the Europeans play a leading role here?

Having concrete strategies in the space domain has never been more important. This is one of the major conclusions the Debating Security Plus online community reached during this debate.

What do the experts think?

Cassandra Steer, Consultant specialising in space security and space laws, argued that framing space as a futuristic frontier hinders us from seeing what it truly is: a current security threat. Steer continued by noting that outer space is "already a part of our natural environment, and already a domain in which we operate militarily and commercially".

Jana Robinson, Senior Fellow at the Prague Security Studies Institute, called out potential hybrid threats such as directed energy operations, jamming and proximity operations, warning that it could endanger our cyber, economic and financial sectors. She further cautioned against Chinese and Russian space-related state-controlled enterprises, which are driven by strategy rather than commercial motives when partnering abroad. Investments in space activities with such enterprises risk being unsustainable for partners and could negatively affect dependent countries.

Russia and China also represent military threats for space governance. **Kaitlyn Johnson**, Associate Fellow and Associate Director for Aerospace Security at the Center for Strategic and International Studies, highlighted Beijing's annual anti-satellite weapons (ASAT) tests and Moscow's "wide-reaching jamming operations in the Arctic circle" which, in the past, have hampered Nordic countries' military and commercial operations.

"It is undeniable that matters of space and security are deeply intertwined. We cannot take these issues for granted and we can only protect ourselves by working together and allocating the necessary resources"

Pedro Duque, Spanish Minister for Science, Innovation and Universities, and former astronaut

What about Europe?

Spanish Minister for Science, Innovation and Universities, and former astronaut, **Pedro Duque** shared his vision of a space strategy for Europe based on coordination between the European Union, the European Space Agency, and member states. Duque believes that while space brings many opportunities, Europe must step up to ensure the safety and security of its citizens from emerging threats in space. “It is undeniable that matters of space and security are deeply intertwined. We cannot take these issues for granted and we can only protect ourselves by working together and allocating the necessary resources.”

The European Space Agency's (ESA) Head of Security **Stefano Zatti** emphasised the shift in what these challenges are, from potential intruders that could damage expensive infrastructure to current cyber threats that can deactivate security systems and alter space activities.

What’s the way ahead?

Guillem Anglada, Reader in Astronomy at Queen Mary University of London and European Young Leader (EYL40), argued against conflating the EU’s ‘space policy’ with the ESA, insisting that the two should be viewed as distinct entities. Rather, Anglada called for the implemention of common EU regulations and protections against outside competition. He also noted that space is the “only place” where unbound exploration can occur without further damaging our planet. Indeed, energy and noble metals found in space could prove a tremendous asset back on Earth.

LGBTQI+ rights in the security sector

Introduction

For many years Women in International Security, which now has chapters all over the globe, performed sterling work in promoting the position of women in the armed forces and in the middle and senior ranks of foreign and defence ministries and international organisations. So, the question is whether a similar approach is what is needed to give equal opportunities to LGBTQI+ people. Their rights are being increasingly recognised and they are taking their place in our armed forces and security establishments as well.

Yet we have experienced a major setback in the United States with President Trump banning LGBTQI+ people from serving in the US-armed forces, thereby reversing the decision of his predecessor, and going against the advice of his own advisors who saw no reason or evidence that LGBTQI+ servicemen and women perform any less well than their heterosexual and cis-gender counterparts. This decision demonstrates the degree of myth making, prejudice and wilful manipulation that still surrounds the LGBTQI+ issue, and underlines the gap still existing between the recognition of their rights – as well as those of women or ethnic or religious minorities – and other groups in society.

Why has the integration of LGBTQI+ people in the security community lagged behind that of other groups? What are the obstacles that specifically apply to LGBTQI+ people and why have they arisen? Where are the good examples and best practices that can be mainstreamed throughout the NATO and EU security establishments and in other Western countries? How can we develop a narrative for the value and role of LGBTQI+ people in international security? What role can LGBTQI+ people and support groups play themselves in developing and promoting this narrative?

While some do not consider the provision of human rights and fundamental freedoms for LGBTQI+ people in the security sector central to national security, Friends of Europe and EUROMIL reiterate our support for a more inclusive security sector which is open to those who are willing and able to serve. We have been pleased to host this important debate together and we will continue to promote LGBTQI+ rights in the future.

What do the experts think?

Alex Araujo argued that if we still treat this issue as a taboo, narratives explaining the value of including LGBTQI+ people in international security efforts will not appear. “People need to be sure that they will not be persecuted, that they will not be victims of prejudice. A lot of people have it. If there is a policy that demonstrates that they will be treated with whatever isonomy the public sector should meet, they would open up and the narratives would appear. We need to treat the issue with more respect for the people of the LGBTQI+ world.”

Freddy Van Eeckhout, Diversity Coordinator at Belgian Defence and Co-Founder of the Belgian Defence Rainbow Community, explained that although Belgium’s armed forces have accepted sexual and gender orientation protections policies in 2010 and 2014 that does not mean that the mentality of organisations has changed and that LGBTQI+ persons have since experienced greater acceptance from their colleagues. Therefore, he encourages the creation of more LGBTQI+ networks because “the more networks that exist and the more people or members of LGBT networks there are, the more difficult it would be perhaps later to make us disappear.”

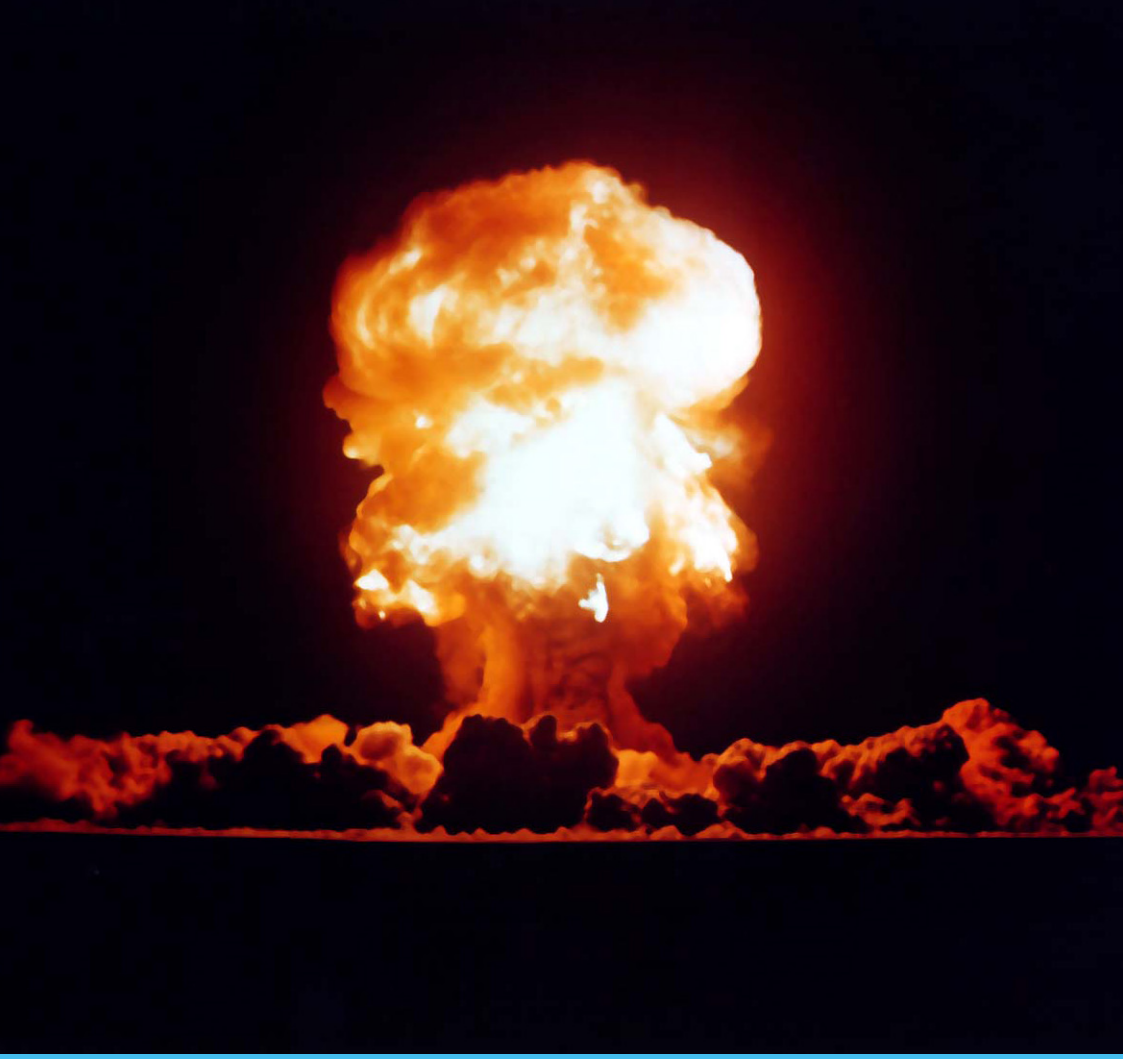
Captain James Carrahar, a British Armed Forces officer, argued that real value comes from having a diverse team. He explained that the British Army’s prestige around the world

"The more networks that exist and the more people or members of LGBT networks there are, the more difficult it would be perhaps later to make us disappear"

Freddy Van Eeckhout, Diversity Coordinator at Belgian Defence and Co-Founder of the Belgian Defence Rainbow Community

for being an effective fighting force will reflect well on its status as an inclusive force, in turn highlighting the fact that diversity provides strength rather than undermines it.

Fidelma Ashe, a member of the Transitional Justice Research Institute at Ulster University, reminded us that LGBTQI+ rights should not only be considered when building our security forces but must also play a key role during peace processes. “Political conflict invariably exacerbates pre-conflict sexual and gender inequalities. The historical trend has been to exclude these inequalities and the harms they engender in peace agreements. Only seven peace agreements provide for some form of equality protection on grounds of sexual orientation and/or gender identity. A peace-building agenda that includes and places a premium on sexual and gender equality helps support a post-conflict ethics of inclusion, diversity and difference. It helps shape a vision of peace that is positive for the entire society”.



Nuclear proliferation and non-state actors

Introduction

Nuclear weapons are back at the top of the international security agenda. Notwithstanding efforts to ban these weapons entirely, there are no signs that the nuclear powers are ready to give their weapons up. Indeed, the recent US national nuclear posture review links the threat of nuclear retaliation to many types of non-nuclear aggression, including by cyber-attacks. Meanwhile, Russia continues to deploy new generations of nuclear-capable missiles in the vicinity of NATO. Iran has resumed nuclear enrichment and North Korea test-fires short-range missiles virtually every week. Following the demise of the Intermediate-Range Nuclear Forces (INF) Treaty the US has tested its first intermediate-range cruise missile for over 30 years and has refused to endorse a 'no first use' principle.

Unlike terrorists operating rudimentary weapons or cyber hackers using computer code, nuclear weapons are big and costly things that require significant research and production infrastructure, as well as testing, delivery systems and secure storage. Hence, these weapons have traditionally been the monopoly of states trying to deter or coerce other states.

Yet, in so many other areas of international security, non-state actors have succeeded in gaining access to destructive technologies that used to be the preserve of states. ISIS has used drones and chemical weapons extensively in Syria. This year, Italian police discovered that a Far Right group had acquired a surface-to-air missile. Even if they do not possess autonomous nuclear capabilities, non-state actors have been active in technology transfer, trafficking in stolen nuclear materials and providing nuclear weapons blueprints and know-how.

When the Pakistani scientist, Abdul Qadeer Khan, was exposed for selling these blueprints to states such as Libya the then head of the International Atomic Energy Agency, Mohamed ElBaradei spoke of a "nuclear Walmart" of horizontal proliferation across the globe. When US intelligence agencies accessed computer drives used by al-Qaeda in Afghanistan they discovered that this terrorist organisation was looking at acquiring nuclear capabilities. Given the assumption that terrorists would be less inhibited about using nuclear weapons compared to states, former US secretary of state, Condoleezza Rice, spoke of "putting the worst weapons into the hands of the worst people".

Is it only a matter of time before a terrorist organisation like ISIS or al-Qaeda acquires a nuclear weapon? What are the current weaknesses in international non-proliferation efforts targeted on non-state actors? In the current atmosphere of tension between nuclear states, can these states still summon the will to limit proliferation to others? Would the nuclear powers ultimately have to agree to give up their own nuclear weapons – through for instance mechanisms such as the UN nuclear ban treaty

– as the price for preventing non-state actors acquiring these weapons?

Our Debating Security Plus discussion on nuclear proliferation and non-state actors brought together experts, policymakers and civil society organisations to discuss these questions and many more.

What do the experts think?

Whilst a large-scale nuclear attack has yet to be carried out by non-state actors, **Elena K. Sokova**, Executive Director of the Vienna Center for Disarmament and Non-Proliferation (VCDNP), argued that terrorists may not need actual materials. Rather, they merely need to trick the opposition into believing they have nuclear weapons to provoke a very real response from their adversary.

William Potter, Director of the Center for Nonproliferation Studies at the Monterey Institute of International Studies, argued that the terrorists' "best ally" is "complacency". That is to say, a lack of concern about the security of nuclear test sites and materials could pose a real danger. Ian Anthony from the Stockholm Institute of Peace Research (SIPRI) argued that a crucial but underappreciated distinction to make is between non-state actors that act with intent and those that are unwitting members of a trafficking network, both of whom can destabilise the nuclear environment.

How exactly should governments respond to the threat of WMD attacks from non-state actors?

Many participants highlighted the importance of multilateral institutions such as the United Nations and the International Atomic Energy Agency (IAEA). **William Alberque** the Director of the Arms Control, Disarmament and WMD Non-Proliferation Centre at NATO, argues that existing conventions on non-proliferation need

"Existing UN conventions must be constantly attended to and kept fit for purpose in a rapidly changing context"

Izumi Nakamitsu, UN Under-Secretary-General and High Representative for Disarmament Affairs

to go further. NATO could play a constructive role in promoting non-proliferation.

However, **Izumi Nakamitsu**, the UN Under-Secretary-General and High Representative for Disarmament Affairs, warned of a collapsing consensus around nuclear non-proliferation and called for innovative new solutions to ensure compliance. She explained that existing UN conventions "must be constantly attended to and kept fit for purpose in a rapidly changing context." **Cornel Feruță**, Acting Director General of the International Atomic Energy Agency (IAEA) argues that in the face of growing amounts of nuclear material globally, the IAEA is training thousands every day on nuclear security issues, at the front line of non-proliferation efforts.

Rolf Mowatt-Larssen, Senior Fellow at the Harvard Kennedy School's Belfer Center recommended the creation of a dedicated capability, under UN purview, focused on preventing WMD terrorism. He also called on states to pool intelligence and law enforcement efforts. **The Russian Permanent Representation to NATO** argued in favour of reviving the NATO-Russia Council to deal with the issue.

Others, however, claim that the problem is more structural. Activist and Director of the International Campaign to Abolish Nuclear Weapons **Beatrice Fihn** insisted that as long as nuclear weapons are considered desirable and valuable as security assets by states and disarmament is not prioritised, non-proliferation efforts will not be successful.

AI in defence

What would a code of conduct for AI look like?

Introduction

Military affairs have always been dominated by technological advances. Sometimes this has been incremental, giving an existing technology a longer lease of life. Yet occasionally, progress is revolutionary and transformative, giving the side that develops the new technology first a significant military advantage over its adversaries.

More recently, the creation of new military domains in cyberspace and outer space has started the debate anew as to whether technology could give a military force a 'Pearl Harbour' effect. This said, history shows that many factors explain victory or defeat and wonder weapons are rarely the key element in this equation. It may be worth recalling this complexity at the very moment that the strategic community is grappling with another potential game changer in military affairs: artificial intelligence (AI) and the speed at which it is spreading into weapon systems, command and control and intelligence, information, and knowledge acquisition.

We need to understand the impact of AI both as a technology but also as a public policy question. As with all potentially revolutionary technologies, it is not simply a matter of exploiting them as fast as possible, both to disrupt adversaries and to prevent these same adversaries from using these technologies to disrupt us. AI presents a number of major public policy questions which need answers before the technology acquires a life of its own.

One issue is the superhuman speed and autonomy of decision-making. An AI-enabled command and control system linked to autonomous weapons systems might decide to open fire in a way that leaves no time for diplomacy.

Another issue is the reliability of AI-driven systems manipulating vast amounts of data but which could be hacked and redirected in ways which human operators are slow to recognise and control. If certain military powers hide their AI capabilities from their adversaries, the incentive will be to mislead your opponent to gain an advantage. This is bound to fuel suspicion and worst-case scenarios. So how can we devise confidence building measures or greater transparency regarding AI-enhanced capabilities, even if formal arms control agreements do not seem feasible?

Finally, consider human control and safety. It doesn't seem sensible to leave warfare to computers that can take decisions according to different criteria than those used by humans. In an increasingly automated battlefield, where should the interface between human and machine lie?

Artificial intelligence in security and defence is developing at lightning speed and the international community must quickly catch up with technological advances if it is to regulate the use of AI on the battlefield. This was the premise of the Debating Security Plus discussion on AI and defence.

What do the experts think?

Courtney Weinbaum argued that an AI 'code of conduct for defence' should draw from other defence codes of conduct and extend the principles of the UN Declaration of Human Rights and the Geneva Convention.

Paul Nemitz, from the Directorate-General for Justice and Consumers of the European Commission argued for the necessity of constraining the use of AI for military purposes from development to deployment and use.

Zhanna Malekos Smith put forward a 'warrior-in-the-design code of conduct' for the armed forces, whereby humans would always verify targets prior to AI engagement. This code of conduct would integrate AI and armed robots to enhance, rather than supplant, human capability in combat.

Rod Thornton instead drew attention to the need for more trust in the international system, stressing that distrust could fuel the emergence of a 'doomsday' AI weapon. He warns that political leaders will not want to seem irresponsible and put their citizens at risk by limiting their own development of AI weapons if other states cannot be trusted to do the same.

What role does Europe play?

Olli Ruutu, Deputy Chief Executive of the European Defence Agency (EDA), presented the EDA's efforts to develop common European guidelines on the use of AI for military purposes.

"Europe can make a contribution to reach consensus on possible standards and regulations on a global scale"

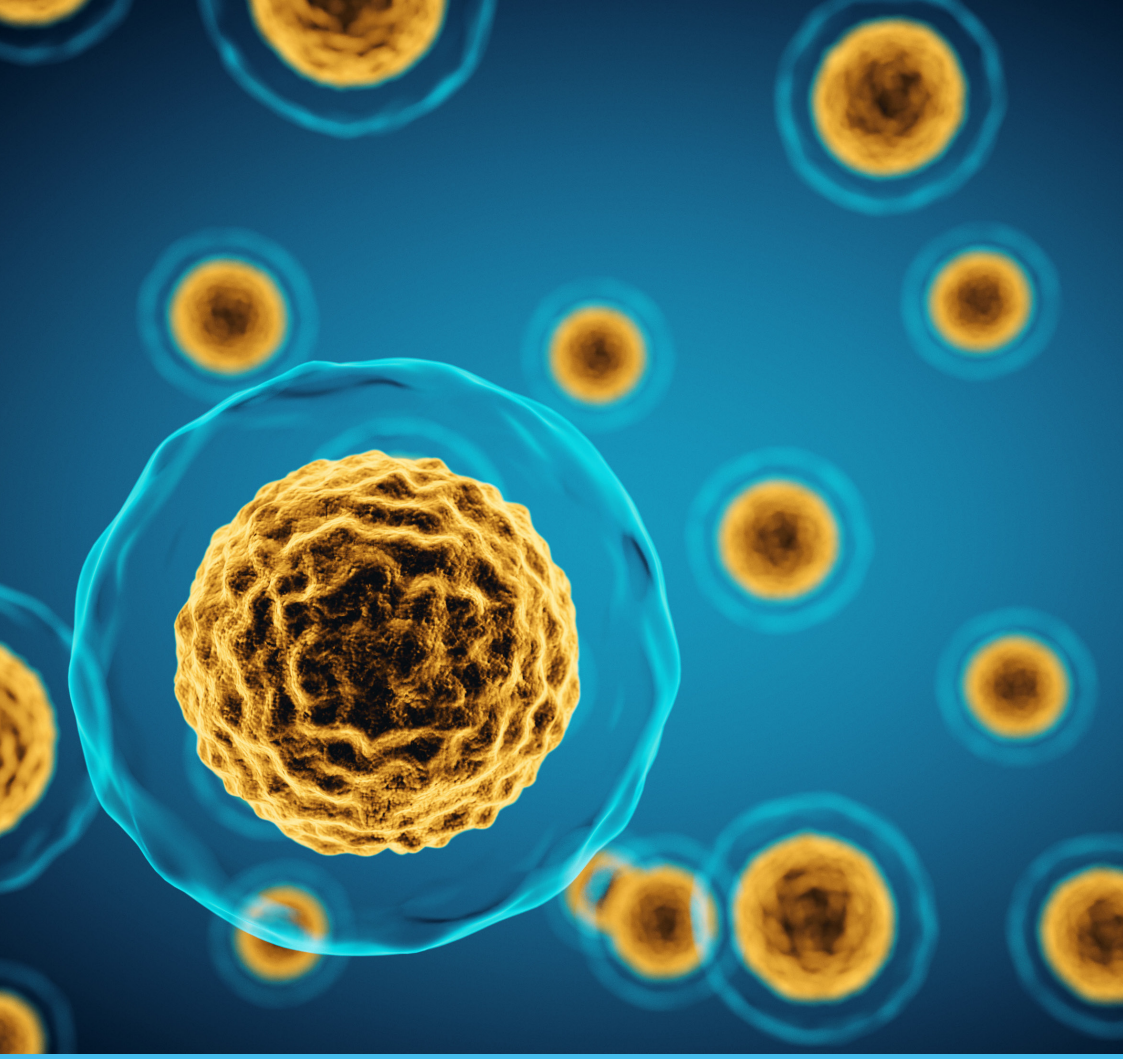
Olli Ruutu, Deputy Chief Executive of the European Defence Agency (EDA)

It currently oversees 30 collaborative projects related to artificial intelligence. “Europe can make a contribution to reach consensus on possible standards and regulations on a global scale.” Yet Estonia’s Ambassador to the EU Political and Security Committee, **Rein Tammsaar**, called on the EU to do even more and triple AI investment. He argued “overregulation and restrictions can undermine exploitation of AI in the defence field, including vis-à-vis other actors not constrained.”

What’s the way ahead?

Hugh Gusterson’s intervention contrasted with many of the other contributions, making the hard-hitting argument that AI technologies, like bioweapons and landmines, should be banned altogether on the battlefield. On autonomous drones he contends that “Western powers may be the first to deploy them, but they will not be the last. If we create them, they will spread.”

Raluca Csernatoni of Carnegie Europe advocated the need for a shift in narratives, nuancing the debate away from either hype about AI revolutionising warfare or crippling anxieties over its potential damaging consequences. He warned that framing the debate as an arms race could cultivate an “insecurity strategic culture premised on antiquated Cold War rhetoric.”



Hybrid warfare and biological agents

Introduction

For many years the threat of the use of biological weapons seemed to have receded. In the 1970s the Biological Weapons Convention (BWC) was agreed and became a quasi-universal UN treaty. Unlike the earlier Geneva Protocol of 1925, the BWC outlawed not merely the production but also the use of biological agents. Like its nuclear counterpart, it seemed to mark a step forward in building legal barriers against any use of these terrifying weapons of mass destruction, although it still lacks a verification mechanism.

The Russian use of the Novichok nerve agent in Salisbury in March 2018 stung the NATO allies and many other countries into action. NATO and the EU immediately initiated a review of their preparedness to respond to Chemical, Biological, Radiological and Nuclear (CBRN) threats, an area that had been much neglected since the end of the Cold War. In both military and civil domains, many gaps needed to be plugged and quickly.

First is the requirement to identify chemical and biological substances rapidly so that we can distinguish between a major flu outbreak and a deliberate biological weapon attack. To help here, NATO has established a Centre of Excellence in the Czech Republic with a reach-back facility to facilitate the notification and laboratory analysis of biological incidents. Yet do we have an adequate system of reporting and early warning of outbreaks in civil contexts such as occurred in Salisbury?

The second area concerns initial response. In the military area, our national authorities are once again standing up CBRN battalions with the protective clothing and decontamination equipment to operate in affected areas on the battlefield. The NATO Response Force has such a standby unit at a high state of readiness. Such military units can support civil contingencies as well; but again, do we have enough of these capabilities in the police, border forces and disaster management agencies to cope with a major attack in a populated environment?

The third area is civil preparedness in the longer term. The Ebola outbreak in West Africa underscored Europe's vulnerability to cope with an epidemic on the scale of Ebola should it spread to our continent. As an epidemic or pandemic of disease is similar to a biological attack the capacity of hospitals and the public health system to surge its capacity quickly is a concern. Our governments and authorities have to be able to detect, respond and mitigate attacks and incidents using these substances. They need to be able to prevent panic and disorder, and to restore basic services as quickly as possible. How prepared are we, how must we improve, and how quickly?

Our Debating Security Plus discussion on hybrid warfare and biological agents gathered experts around the globe to discuss these questions and many more.

What do the experts think?

Filippa Lentzos, Senior Research Fellow at Kings College London launched the debate by arguing that we should not think of bio-weapons as we do of bombs, "they are processes rather than items". Dr Lentzos warned that a side effect of increasing numbers of countries developing bio-defence programmes is also an increasing capacity to do harm in the biological sphere, and an increased chance that this capacity to harm could turn into a threat, should the intent be there. "While there may not be reporting that any countries are maintaining biological weapons programs, we are seeing worrying signs of build-ups in capacity."

Preventing an escalation is thus crucial. Concrete measures can be taken to ensure that bio-threats are addressed before a potential attack. **Peter McGrath**, Coordinator of the InterAcademy Partnership, highlighted the importance of working across borders to establish consensus among scientists, raising awareness of dual-use issues in biotechnology, particularly across the developing world. McGrath's organisation is at the forefront of operationalising the promises of the BWC and preventing an unintentional escalation.

Helge Martin of the University of Hamburg outlined three key ways that states could enhance their preparedness for a bioweapons attack; strengthening local health systems, strengthening inter-agency cooperation to address the health-security nexus and strengthening the coordination of international

"While there may not be reporting that any countries are maintaining biological weapons programs, we are seeing worrying signs of build-ups in capacity"

Filippa Lentzos, Senior Research Fellow at Kings College London

assistance to prevent the delays that hampered the international community's response to the West Africa Ebola Crisis.

What role can the private sector play in establishing preparedness against bioweapons attacks? **Daniil Davydoff**, Associate Director of Intelligence at AT-RISK International, contends that whilst vulnerabilities in the biosecurity sphere are growing, they tend to be neglected by stakeholders in the private sector. Davydoff warns that only the deployment of military-grade bioweapons is taken into account by companies in their risk analyses and not wider background bio-threats such as vectors spreading globally and antimicrobial resistance worsening.

Internet governance and cyber security

Introduction

Eric Schmidt, the former CEO of Google, used to quip that the Internet is the first thing mankind has invented that it cannot understand. Certainly the advent of cyberspace introduced us to a new age of hyper-connectivity and therefore of complexity. We have been grappling with its consequences ever since. Cyberspace has connected people across the globe. As open cyberspace is (still) a global phenomenon: any local cause rapidly becomes national and even international, as we have seen with opposition to vaccinations, right-wing populism and jihadist groups. Cyberspace is the domain of ideas but also of fund-raising, recruitment, logistics, business operations and battlefield planning.

As a result, cyberspace has acquired a strategic value in addition to its ever-pervasive societal and economic roles. It has become a military domain of operations in its own right. Man-made cyberspace now holds the key to vital military functions such as data storage, retrieval and analysis communications, navigation positioning, and command and control. This massive dependency has led some to wonder whether wars could be won or lost exclusively in cyberspace.

Cyberspace has created a new set of vulnerabilities, most hidden. As mainly commercial, off-the-shelf technology is used, security has to be expensively retrofitted. As cyber-attacks become more sophisticated and attract state level hackers, outright denial of service attacks are being superseded by more insidious forms of cyber intrusion where data can be manipulated rather than simply stolen. This could lead commanders to lose faith in their own command and control systems.

Yet despite these difficulties, cyberspace is also an attractive domain for political leaders and commanders. It can achieve results more cheaply than using a conventional weapon. It can be more easily denied which makes it ideal for covert operations and sending signals short of war. It is also an excellent means of espionage, to probe an adversary's weaknesses. Over 30 countries are believed to have serious offensive cyber capabilities and many have established military cyber commands.

The question is whether to use these weapons in the hope of prevailing or to limit them through arms control agreements based on collective restraint. But can the latter work realistically in a virtual domain like cyber, where we are dealing with millions of computers, cables and servers and not just a limited, observable number of tanks, missiles and aircraft? How successful have organisations such as the EU and NATO been in lowering the vulnerability of their member countries? Are member states ready to assist each other or to develop a comprehensive set of responses to deter and respond to cyber-attacks? How bad does a cyber-attack have to be before it can be considered as the equivalent of an armed attack? And what then would be an appropriate response?

There has never been a more pressing need to establish an international code of conduct for cyber space and build capacity against cyber-attacks worldwide. Preserving the openness of the Internet as well as building resilience against offensive actions in cyberspace were key priorities among participants in the final Debating Security Plus discussion of 2019.

What do the experts think?

Despina Spanou, for Digital, Trust and Cyber Security drew attention to the problem of disinformation campaigns and cyber-attacks in violating the integrity of elections across Europe. Ms Spanou highlighted the importance of European-wide measures that cross public/private sector boundaries and using new technologies such as Artificial Intelligence to counter this threat. "…protecting not only our systems but also our societies, our democracies, our fundamental rights, we do not keep this only for the borders of the internal market of the European Union. These are also the underlying principles for our global diplomacy…"

"…Protecting not only our systems but also our societies, our democracies, our fundamental rights, we do not keep this only for the borders of the internal market of the European Union. These are also the underlying principles for our global diplomacy…"

Despina Spanou, Head of Cabinet for European Commission Vice President Margaritis Schinas

However, no country or region can prevent cyber-attacks on its own. **Tobias Feakin**, the Australian Ambassador for Cyber Affairs, argued that cyber diplomacy plays a critical role in preventing countries from pushing the boundaries of what is acceptable in cyberspace and building the cyber capacity of countries to promote a high-standard of global cyber security. He argues that WannaCry and the NotPetya incident "are two good examples of where we have come together as an international community and said this is unacceptable." **Vytautas Butrimas**, a cyber security expert, suggested that the international community could adapt the model of the Convention Prohibiting the use of Chemical Weapons and the organization of the same name to monitor and report on violations in cyberspace. Yet **the Russian Mission to NATO** argued that

a convention to combat crimes in cyberspace should take into account interests of all countries and be based on the principles of sovereign equality and non-interference.

Francesca Musiani, researcher at the Centre national de la recherche scientifique (CNRS), drew attention to a wider threat to good internet governance: Russia's recent pledges to cut itself off from the rest of the World Wide Web. She argued that beyond the symbolic significance of Russia's 'sovereign internet law' and empowerment through disconnection, such attempts should not be made for the sake of the Internet on an international scale.

But what challenges do existing efforts face in establishing a more secure Internet?

In response to Despina Spanou, **Christer Hammarlund** from the European Commission highlighted that cyber security legislation should address the causes behind the cyber-attacks rather than the effects, recommending that in the future no Internet of Things devices can be sold and installed on our networks, unless they have built-in cybersecurity details to minimise vulnerabilities. **Malcom Warr**, Member of the Cyber Expert Group at the Scottish Business Resilience Centre responded that whilst technological resilience is important, taking a bottom-up 'Current in the Bun' approach and embedding cyber professionals at all levels and countries in NATO efforts is imperative.

Some participants voiced concern about existing offensive cyber capacity. **Max Smeets**, a senior researcher at Stanford University highlighted the problem of NATO allies being unable to mount effective offensive cyber operations when they do not agree on the appropriate procedures and boundaries. To remedy this, he recommends that NATO allies should establish memoranda of understanding on offensive cyber operations in systems or networks based in allied territory.

Ultimately, we may need a clearer idea of what a cyber peace should look like. **Scott Shackelford**, Professor at Indiana University argues that the key lies in focusing on a more positive vision as digital conflict and military action are increasingly intertwined. This approach would include better governance, respect for human rights, making internet access more widely available around the world, and teaching everyone how to protect themselves online.

Friends of Europe
Connect. Debate. Change.

+32 2 893 98 12
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.