Final Report:

The Implications of Military R&D in Key Emerging and Disruptive Technologies for Transatlantic Cooperation

17 June | Bush House, London

M. Bekkers, A. Bumpers, R. Csernatoni, S. Daultrey, K. Floyd,
T. Lawrence, T. Longo, E. Marcus, P. Pernik, K. Tucker

The Implications of Military R&D in Key Emerging and Disruptive Technologies for Transatlantic Cooperation

Authors: M. Bekkers, A. Bumpers, K. Tucker
Editors: R. Csernatoni, S. Daultrey, K. Floyd, T. Lawrence, T. Longo, E. Marcus, P. Pernik

WILLIAM & MARY
CHARTERED 1693
CCDCOE
NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE
UNITED STATES MISSION
NORTH ATLANTIC TREATY ORGANIZATION
CARNEGIE EUROPE
KING'S College LONDON

Table Of Contents

Foreword

Divergence in visions and strategies for military technological innovation between the U.S. and NATO Member Nations, especially in Europe, significantly impacts transatlantic cooperation. As Emerging and Disruptive Technologies (EDTs) – such as AI, quantum computing, and advanced robotics – increasingly shape global security, the competing approaches to dual-use and military R&D within the Transatlantic Alliance create challenges for cohesive policy-making and joint innovation efforts. The U.S. and Europe have different priorities, funding mechanisms, and strategic objectives, leading to potential misalignments in how technologies are developed, deployed, and integrated into military operations. Against the backdrop of an evolving geopolitical landscape and the ongoing Russo-Ukrainian war, this divergence poses risks to the effectiveness of Transatlantic defence and security cooperation.

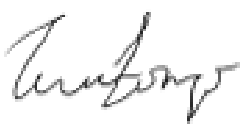
This one-day workshop examined competing visions of military technological innovation, focusing on how these influence industrial and technological innovation policies on both sides of the Atlantic. By unpacking differences and commonalities, attendees from the military, government, industry, academia, and more identified opportunities for greater alignment and collaboration, contributing to more coherent and effective transatlantic military cooperation.

This workshop was the next step in a deep and enduring partnership between NATO's Cooperative Cyber Defence Center of Excellence (CCDCOE), King's College London, and Carnegie Europe, with support from the U.S. Mission to NATO. Funded by the U.S. Mission to NATO, William & Mary, CCDCOE, and King's College London published "Cyber Threats and NATO 2030: Horizon Scanning and Analysis" in 2020. We followed that with a virtual event until we could gather in October 2022 in Brussels for a workshop on cyber resilience, this time with EU Cyber Direct. At each stage, we have answered the call from the U.S. Mission to NATO to build on novel ideas and approaches and push forward to do more.

Contained in this publication is a summary of the proceedings with key outcomes noted from the Breakout Groups. To allow for maximum discussion and debate, the majority of the workshop operated under Chatham House Rule with non-attribution.

As a global leader in education, William & Mary remains deeply grateful to our co-hosts, collaborators, and the U.S. Mission to NATO for empowering us to help make a safer, more secure world.

Kathryn H. Floyd, Ph.D.
Director
Whole of Government Center of Excellence



Prof. Teresa V. Longo, Ph.D.
Senior International Officer

Workshop Schedule

9:00–9:10	**Welcome Remarks** Prof. Teresa V. Longo, Senior International Officer, William & Mary Dr. Kathryn H. Floyd, Director, Whole of Government Center of Excellence, William & Mary
9:10–9:30	**Opening Remarks** Rodney D. Ford, Minister Counselor for Public Affairs, U.S. Mission to the United Kingdom
9:30–10:30	**Plenary Panel - "Geopolitical Competition in EDT: Implications for NATO and Tech Rivalries"** Fiona Bradley, Chief of Staff, Defence, Palantir Technologies Dr. Joe Devanny, Senior Lecturer, National Security Studies, Department of War Studies, King's College London Dr. Amy Ertan, Cyber and Hybrid Policy Officer, NATO Headquarters Piret Pernik, Researcher, Strategy Branch, NATO Cooperative Cyber Defence Centre of Excellence
10:30–10:45	**Coffee Break**
10:45–12:45	**Breakout Group 1: “Competing Visions of Military EDTs”** Professor Antonio Calcara, Senior Associate, Centre for Security, Diplomacy and Strategy (CSDS), Vrije Universiteit Brussels Dr. Raluca Csernatoni, Fellow, Carnegie Europe Dr. Edward Hunter Christie, Senior Research Fellow, Finnish Institute of International Affairs Dr. Simona Soare, Senior Lecturer, Lancaster University

10:45 - 12:45	**Breakout Group 2: "Alignment Areas of These Competing Visions"** KatyAnn Coulter, Chief, Data Programs Branch ACC A29P, ACC/A29 Data Tech Futures Division, United States Air Force Benjamin Dunlap, Data Operations Branch Chief, United States Air Force/Air Combat Command/A29 Dr. Nathan Fisher, Defence Health Lead, Noblis, Inc. Dr. Kathryn H. Floyd, Director, Whole of Government Center of Excellence, William & Mary Huw Williams, Senior Fellow & Editor, The Military Balance, The International Institute for Strategic Studies
10:45 - 12:45	**Breakout Group 3: "Cyber Threat Intelligence Sharing Between NATO Allies"** Eman Blair, Senior Vice President for Technology Advancement and Special Advisor, Pentagon Federal Credit Union Sally Daultrey, Research Affiliate, Whole of Government Center of Excellence, William & Mary Dr. Andrea Gilli, Lecturer, University of St Andrews Roger Yee, Managing Partner, Outcome One
13:45–14:15	**Breakout Groups Report Out**
14:15 - 14:30	**Closing Remarks** Dr. Kathryn H. Floyd, Director, Whole of Government Center of Excellence, William & Mary

Workshop Co-Hosts

WILLIAM & MARY
CHARTERED 1693

UNITED STATES MISSION
NORTH ATLANTIC TREATY ORGANIZATION

KING'S College LONDON

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

CARNEGIE
EUROPE

Workshop Collaborators

PS21
PROJECT
FOR THE STUDY OF THE
21ST CENTURY

YOUNG PROFESSIONALS IN FOREIGN POLICY

Author Bios

Myrthe Bekkers

Myrthe Bekkers is a Master's student in National Security Studies at King's College London. She is Research Assistant at the Freeman Air and Space Institute in the School of Security Studies, where she contributes to a policy-focused analysis of escalation dynamics in space. Her own research centres around strategic autonomy and Dutch space capabilities in the Armed Forces, maritime autonomy, and disruptive technologies in defence.

Myrthe holds a BA International Relations and International Organization and a BA in Dutch Law from the University of Groningen, and brings experience in commercial law and policy research.

Alex Bumpers

Alex Bumpers is an MA student in the Intelligence and International Security program at King's College London (KCL). His studies examine the intersection of emerging technologies and security. He is particularly interested in cyber defence and public-private innovation partnerships. Previously, he was a Senior Consultant with Guidehouse's defence and Security practice, where he led national security innovation projects for federal clients focused on risk management and national resilience. Prior to that, he supported digital transformation projects at the U.S. Department of State. He earned his BA in History of Public Policy from the University of California, Santa Barbara.

Dr. Raluca Csernatoni

Dr. Raluca Csernatoni is a research fellow, working on European security and defence with a focus on emerging and disruptive technologies like Artificial Intelligence (AI), at Carnegie Europe in Brussels, Belgium. At Carnegie Europe, she is a team leader and senior research expert on new technologies for the EU Cyber Diplomacy Initiative - EU Cyber Direct (EUCD) project and leads Carnegie Europe's research on 'The EU's Techno-Politics of AI'. Csernatoni is currently a professor on European security and defence, focusing on digital technologies, with the Brussels School of Governance (BSoG) and its Centre for Security, Diplomacy and Strategy (CSDS) at Vrije Universiteit Brussel (VUB), Belgium. At the CSDS, she is also a senior research expert on digital technologies in the context of the EU-funded project, 'Indo-Pacific-European Hub for Digital Partnerships: Trusted Digital Technologies for Sustainable Well-Being - INPACE'.

Sally Daultrey

Sally Daultrey is a Research Affiliate at the William & Mary Whole of Government Centre of Excellence, where she collaborates with Professor Chon Abraham on comparative analysis of cyber threat intelligence sharing frameworks, laws and practices in the U.S. and other jurisdictions. With 22 years of on-the-ground experience in 29 countries, she has worked extensively in Central Asia, India, Singapore and the U.S. on science diplomacy and non-traditional security projects. She is based in London.

Dr. Kathryn H. Floyd

Kathryn H. Floyd, Ph.D., is the Director of William & Mary' s Whole of Government Center of Excellence (WGC). The WGC, part of the W&M Military & Veteran Affairs team, serves as a university hub dedicated to all matters of national security: military and interagency training and strategic leader development; convening academics and practitioners on research priorities; and degree-based education.

Floyd received her Ph.D. in Strategic Studies (focusing on pre-radicalization) from S. Rajaratnam School of International Studies, Nanyang Technological University (Singapore) where she worked with the International Centre for Political Violence and Terrorism Research (ICPVTR). She holds an MA in War Studies from King' s College London (United Kingdom) and a BA in Government from William & Mary.

Tyler Lawrence

Tyler Lawrence is the International Events Manager at William & Mary's Reves Center for International Studies. In his role, he plans and manages international events on campus and abroad to help cultivate a global university. Prior to William & Mary, Tyler worked in theater and film event management in New York City. He received his BA in English from George Mason University and his M.Ed. from Old Dominion University.

Professor Teresa Longo

Teresa Longo is the Associate Provost for International Affairs and the Executive Director of the Reves Center. She is also a Professor of Hispanic Studies. She holds a Ph.D. from the University of Wisconsin-Madison and an M.A. and B.A from the University of Montana. Her scholarship focuses on the relationship between Latin America and the United States as it is articulated culturally.

Professor Longo's publications include Visible Dissent: Latin American Writers, Small U.S. Presses, and the Political Imagination; "Humanity Rendered Visible: Literature, Art and the Post-9/11 Imagination"; and Pablo Neruda and the U.S. Culture Industry.

She is the recipient of William & Mary's Thomas Jefferson Award, a Jefferson Teaching Award, an Alumni Society Teaching Award, and a Plumeri Award; she was recognized by the Case-Carnegie Foundation as a Virginia Professor of the Year.

Elizabeth Marcus

Elizabeth Marcus is a 4th-year undergraduate at William & Mary majoring in International Relations and Philosophy. She is the co-president of the William & Mary Global Innovation Challenge (WMGIC), a student-led organization that hosts interdisciplinary case competitions and mobilizes young adults to tackle global issues in security and sustainable development. As a William & Mary Freeman Fellow, Elizabeth is currently interning at the Caucus of Development NGO Networks (CODE-NGO) in Quezon City, the Philippines. Upon graduation, Elizabeth hopes to serve her country overseas in the U.S. State Department.

Piret Pernik

Piret Pernik is a Researcher at the Strategy Branch of the NATO Cooperative Cyber Defence Centre for Excellence (CCDCOE). She is also a Ph.D. candidate at the Military Technologies Department of the National Defence University, Finland since 2024. She has worked in the cybersecurity area since 2013 as a researcher has authored and co-authored numerous research reports and policy analysis, including book chapters, and published in peer-reviewed scientific journals. Prior to joining the CCDCOE in 2019, Piret Pernik was a Research Fellow at the International Centre for Security and Defence (ICDS), Estonia's largest think tank focused on security and defence matters. Between 2003-2013 she served in the Estonian Ministry of Defence in defence policy planning section. She worked for three years as an Adviser of the National Defence Committee of the Parliament of Estonia in 2009-2012. She holds a Master's degree on Social Theory (Sociology), and on International Relations and European Studies from Estonian Institute of Humanities, University of Tallinn and Central European University, Budapest respectively.

Kyle Tucker

Kyle Tucker is a Marshall Scholar pursuing graduates studies in national security and strategy at King's College London and the University of St Andrews. His academic and professional focus is in international security, especially nuclear issues and science and technology policy. Previously, he worked as a Scoville Peace Fellow at the Nuclear Threat Initiative in Washington, DC, and as an intern at the Center for Nonproliferation Studies in Monterey, California. A former Boren Scholar, he also studied the Russian language in Almaty, Kazakhstan. Tucker holds BA degrees in International Studies and Russian from Indiana University Bloomington and is a proud Hoosier.

Opening Remarks

Opening Remarks

Rodney D. Ford, Minister Counselor for Public Affairs, U.S. Mission to the United Kingdom

Rodney D. Ford, Minister Counselor for Public Affairs at the U.S. Mission to the United Kingdom delivered the workshop's Opening Remarks. Mr. Ford began the session by highlighting the importance of the 2025 NATO Summit in The Hague and the urgent need for NATO to improve military cooperation and foster innovation in response to today's evolving security environment. He pointed to the ingenuity of the Ukrainian armed forces, which are leveraging a combination of high and low-tech solutions to reshape the battlefield. Mr. Ford underscored the need to anticipate, rather than react to, shifts in warfare by learning from today's battlefield lessons and deploying emerging and disruptive technologies (EDTs) to strengthen deterrence and broaden security options.

Mr. Ford urged that NATO must evolve in order to remain the world's most successful military Alliance. He emphasised the importance of collective defence investment, applauding the 20+ allies that have increased their spending since September 2024. He argued that raising defence expenditure commitments to 5% of GDP is necessary to ensure that innovation translates into real capabilities. He called for increased investment in emerging and disruptive technologies, stressing the importance of accelerating innovation and incorporating it through streamlined defence acquisition and deployment. From munitions to microchips, he championed deeper transatlantic industrial cooperation and a unified effort across sectors and borders. In closing, the message was clear: NATO must lead, not follow, in evolving to meet the realities of modern conflict.

Plenary Panel

Geopolitical Competition in EDT: Implications for NATO and Tech Rivalries

Plenary Panel - "Geopolitical Competition in EDT: Implications for NATO and Tech Rivalries

- Fiona Bradley, Chief of Staff, Defence, Palantir Technologies
- Dr. Joe Devanny, Senior Lecturer, National Security Studies, Department of War Studies, King's College London
- Dr. Amy Ertan, Cyber and Hybrid Policy Officer, NATO Headquarters
- Piret Pernik, Researcher, Strategy Branch, NATO Cooperative Cyber Defence Centre of Excellence

The workshop's plenary panel reached a consensus that technological innovation is a strategic necessity for NATO and risks must be taken to retain an edge in a world of greater geopolitical competition. However, NATO's procurement processes for emerging and disruptive technologies are widely viewed as slow and ill-suited for the pace of innovation required. NATO programs like the Rapid Adoption Action Plan (RAAP), the Defence Innovation Accelerator for the North Atlantic (DIANA), and NATO Innovation Fund (NIF) are seen as promising mechanisms to improve interoperability and streamline procurement timelines, but there are concerns these efforts are not achieving enough. All participants agree — the challenges to NATO cohesion are known, but implementing long-term solutions remains difficult.

Although no panacea exists, innovation and development of new dual-use technologies, especially those relating to Artificial Intelligence (AI), can help relieve capacity shortfalls. However, the dependence of the commercial viability of emerging defence technologies on civilian market traction has widened the innovation gap between both sides of the Atlantic. Member states recognise that the budget for defence innovation should increase, but questions about which defence capabilities to specialize in and how to make them interoperable between members of the Alliance remain. Too much development in sovereign AI capabilities, for example, could harm NATO interoperability, while over-regulation and lack of standardization can stifle innovation, especially in digital systems. "Minilateral" collaborations between a small group of states, such as the AUKU.S. partnership, were suggested as a potential path forward enabling countries to develop and adopt military AI at different speeds.

NATO is undergoing a generational funding priority shift in its capabilities as new technologies rapidly emerge. Facilitating an environment that encourages defence innovation by including industry partners and creating opportunities to experiment was widely agreed upon. Such an environment avoids over-reliance on singular technologies, capabilities, or private industry partners and gives all member states a chance to participate in innovation. While NATO mechanisms like DIANA and RAAP are imperfect, they still seek to allow for measured risks in financing defence innovation. The plenary panel agreed that rapid innovation and adoption of emerging technologies is necessary, but will need to strike the right balance between improving capabilities and maintaining Alliance cohesion.

Breakout Group 1

Competing Visions of Military EDTs

Breakout Group 1: Competing Visions of EDTs

- Professor Antonio Calcara, Senior Associate, Centre for Security, Diplomacy and Strategy (CSDS), Vrije Universiteit Brussels
- Dr. Raluca Csernatoni, Fellow, Carnegie Europe
- Dr. Edward Hunter Christie, Senior Research Fellow, Finnish Institute of International Affairs
- Dr. Simona Soare, Senior Lecturer, Lancaster University

Rapporteur: Myrthe Bekkers, Student, King's College London

NATO's member states are pioneering advanced military EDTs across a range of joint warfighting functions, including intelligence, situational awareness, and command and control. While major NATO players heavily invest in cutting-edge dual-use EDTs, less-resourced allies struggle to keep pace. As this group discussed, this disparity brings challenges to a cohesive technology strategy. The challenge lies not in divergent priorities, but in operationalising shared objectives across NATO's diverse national contexts.

Competing Visions and Strategy

As a starting point for the conversation, the group observed that member states generally agree on the importance of EDTs for the modernisation of the armed forces. Allies identify similar key technologies in policy documents, agree on the need to engage with the commercial sector, and prioritize a 'whole of nation' approach. At the same time, notable differences remain, reflecting divergent national priorities, ambitions, and risk tolerance. This divergence is further complicated by the U.S. prioritising China as a security challenge, while the European allies focus on Russia. Europe has traditionally relied on the U.S. for defence, but there is a growing recognition of the need for greater European autonomy, especially when U.S. commitment wanes. However, this autonomy should not be absolute. While greater autonomy for European states needs to be the central focus, there should be an equal emphasis on NATO cohesion, with France mentioned as an example of a member that balances these priorities.

Interoperability

Interoperability remains a persistent challenge within NATO, exacerbated by disparities in technological investment, capabilities, standards, and access to cutting-edge technologies among member states. The fragmentation of the European defence industry due to differing national budgets and priorities hinders cohesive modernisation and the integration of EDTs. As highlighted above, efforts like DIANA and NIF aim to address these gaps. While the effectiveness of these initiatives is debated, participants noted that both show definite successes, and their establishment within an intergovernmental collective defence organisation is itself a significant achievement.

Cultural dynamics and the human factor

Panelists highlighted that military research and development (R&D) cultures differ significantly between the U.S. and Europe. The U.S. is seen as a lead innovator, while European countries often perceive themselves as optimisers or technology regulators. A crucial point that participants touched upon was that cultural and organisational factors, rather than just procurement or funding, are major barriers to innovation in Europe. While access to sufficient funds is critical to innovation, participants highlighted that having the right people is at least equally important. Social and political culture, including public opinion and generational attitudes, play a crucial role in preparing for and implementing military innovation. Fostering the attitudes and skillsets that contribute to innovation requires civic engagement, especially with younger generations.

Innovation

To further foster innovation, procurement processes need to be more adaptable and inclusive of commercial providers, particularly subject matter experts (SMEs). Simultaneously, however, there is scepticism about replacing traditional defence primes with numerous startups, as integration and collaboration remain challenging.

Rather, it was suggested that the integration of EDTs into defence requires new approaches to contracting and collaboration between primes and smaller firms. There is a recognised need to accelerate open innovation models that engage all stakeholders – commercial partners, academia, and startups – rather than relying solely on government-driven 'pipeline innovation'.

Cutting-edge innovation occurs in countries such as France, the Netherlands, Germany, Finland, and the United Kingdom, but in scaling and transition there remain critical gaps. There is generally a low risk appetite in procurement, and insufficient planning for horizontal integration across nations. The narrative that 'regulation hinders innovation' is counterproductive: structured planning for innovation transition is essential. Furthermore, while NATO allies broadly agree on the strategic advantages of EDTs, their varying impact and readiness for battlefield use requires nuanced, domain-specific approaches for their integration to ensure that interoperability is not complicated, rather than simplified, by new technologies, especially in contested environments.

EU-NATO Synergy

Finally, it was highlighted that collaboration between the EU and NATO is improving but remains dependent on national governments. The structures are naturally complementary: the EU's legislative and budgetary powers offer opportunities for shaping defence markets, while NATO focusses on standards and soft coordination. Coherence can be engineered among the 23 states that are members of both organisations. Especially at the EU level, policy discussions are evolving, and strong leadership is emerging from countries like Germany. However, EU member states need to demonstrate their commitment by providing the necessary funding.

Participants showed a mix of optimism and pessimism about cooperation and future governance regarding EDTs. While structures and initiatives are in place, significant gaps remain in planning, execution, and cultural adaptation. The core question is not whether to invest in EDTs, but how to do so effectively, ensuring innovation is planned, scalable, and integrated across the entire Alliance. Ultimately, bridging these gaps will require sustained commitment and a common vision to turn ambition into operational advancement for NATO as a whole.

Takeaways:

- NATO Allies share a unified vision for integrating advanced EDTs, but significant challenges remain in operationalising this ambition due to disparities in resources, innovation cultures, and interoperability.
- Integrating EDTs across NATO will require sustained commitment, improved planning and execution, adequate funding, and willingness to share risks.

Outcomes: Identification and analysis of competing visions for military technological innovation between the U.S. and NATO Member nations, focusing on EDTs.

1. Major NATO members pursue heavy investment in emerging and disruptive technologies (EDTs), while less-resourced allies struggle to keep pace.
2. Cultural attitudes towards risk and disruption vary: Europe leans toward optimization and incremental changes, while the U.S. toward bold innovation and radical disruption.
3. Although improvements are visible, defence spending and priorities remain mostly decided at the national level. This results in fragmentation, especially in the EU, where individual countries pursue distinct ambitions - some striving for technological autonomy, others accepting niche roles within U.S.-led coalitions.
4. Different countries within NATO follow different governance models for military R&D, procurement, and collaboration with industry, potentially decreasing Alliance-wide technological readiness, interoperability, and cohesion.
5. The U.S. primarily perceives China as its main security challenge, driving its technological priorities; most European allies focus on Russia.
6. European countries face challenges in rapidly scaling defence investment. Furthermore, although NATO defence spending will increase, some member states remain focused on short-term readiness rather than long-term investments in technology.

Breakout Group 2

Alignment Areas of These Competing Visions

Breakout Group 2: Alignment Areas of These Competing Visions

- KatyAnn Coulter, Chief, Data Programs Branch ACC A29P, ACC/A29 Data Tech Futures Division, United States Air Force
- Benjamin Dunlap, Data Operations Branch Chief, United States Air Force/Air Combat Command/A29
- Dr. Nathan Fisher, Defense Health Lead, Noblis, Inc.
- Dr. Kathryn H. Floyd, Director, Whole of Government Center of Excellence, William & Mary
- Huw Williams, Senior Fellow & Editor, The Military Balance, The International Institute for Strategic Studies

Rapporteur: Kyle Tucker, Student, King's College London and University of St Andrews

This group examined divergent approaches to defence innovation across NATO, particularly between the U.S. and Europe. There was broad alignment in strategic visions and priorities for defence R&D. However, the methods by which objectives are achieved vary significantly. The group concluded that in order to create stronger collaboration and more effective joint operations, NATO must improve the standardization of data and emerging technologies frameworks, support scalable, tactical and local-level experimentation, and dismantle institutional barriers that prevent effective coordination and knowledge sharing across borders.

Defining Visions and Priorities

Participants emphasised general conceptual alignment between European and U.S. approaches to defence innovation priorities. In particular, these priorities include the need to prepare for great-power conflict, leverage secure and agile AI systems, and empower tech-enabled decision-making. There is a decisive need to accelerate the scale and scope of current programmes, with a desire to innovate "on the edge", something that European member states have fallen behind on compared to the U.S.

Central for all member states is the commitment to collaboration and partnership. However, there are cultural differences between approaches to innovation and national security, with the U.S. focused on more practical developments and Europe preoccupied with the strategic and theoretical. Integrating both approaches with industry through an "accelerator" model of development to improve interoperability, communication, and data management was identified as a method to achieve NATO's visions and priorities.

Vision Divergence

Participants candidly identified areas where U.S. and European NATO members misalign, most notably around risk appetite, speed of innovation, and regulatory frameworks. European members operate within stricter data protection and privacy standards, which limits real-time integration of emerging technologies. Furthermore, Europe emphasises deterrence and total defence. The U.S., by contrast, is more inclined to accept risk for speed and combat readiness. While both the U.S. and European NATO partners are concerned about the risk Russia poses to the Alliance, the European view is less hawkish than the U.S. with respect to China as a strategic challenger.

Current NATO frameworks for standardization remain optimized for traditional, large-scale weapons systems and fail to accommodate the commercial, dual-use, and fast-moving nature of emerging technologies such as AI and biotechnology. Export controls, particularly U.S. International Traffic in Arms Regulations (ITAR), were cited as a bottleneck for sharing data. European defence innovation capacity is also limited by European regulations on venture capital, lack of private venture, as well as defence startups working with dual-use technologies. Without a standardized means of handling classified data across the Alliance, innovation is throttled. Increasing standardization can quicken the speed of the procurement cycle.

Areas for Convergence or Alignment

To improve interoperability and collaboration, participants called for the development of consensus-based standards regarding data management and dual-use technologies, especially when commercial development cycles outpace policy adaptation. Standards should accommodate rapid testing and the dissemination of results. All agree on the role of private industry, but harmonizing the U.S. and European approaches will be crucial in building up the capacity for a faster R&D and innovation cycle.

In terms of process, while the sharing of data and best practices should be centralized, experimentation and testing should be delegated to the tactical and state-level, echoing the discussion of "minilateral" relationships during the plenary panel. Furthermore, having greater tolerance for failure in the innovation process is crucial. Promoting replicable lessons learned from the Russo-Ukrainian War and allowing for bottom-up approaches for specialization were also noted. For example, Estonia spearheaded the NATO Cooperative Cyber Defence Centre of Excellence due to its vibrant grassroots cybersecurity community and active support from the Estonian government.

Finally, it was emphasised that while warfighting doctrine in NATO is largely aligned, logistical issues, for example the ability to take a new technology and place it in theatre, are considered a national responsibility and lack integrated planning. Solving this issue through specialization, as well as investing in human capital and an organisational culture supportive of defence innovation in each member state will also assist in unlocking the potential of shared defence R&D and operationalise emerging technologies at scale to meet the current threat environment.

Takeaways:

- Modernize NATO standardization frameworks to support interoperability and adoption of EDTs.
- Reform regulatory and institutional barriers at the state and Alliance-levels to enable faster innovation.
- Scale bottom-up driven innovation and supply chains through minilateral partnerships, localized experimentation, and investment in human capital.

Outcomes: Identification of areas where U.S. and NATO approaches to military R&D can be aligned to foster stronger collaboration and more effective joint operations.

1. Standardization of digital infrastructure and data management.
2. Shared frameworks for the development, integration, and management of EDTs.
3. Harmonization of differences in risk tolerance, threat perception, and innovation culture.
4. Flexible procurement models that permit localized experimentation and voluntary national specialization.
5. Improved coordination of logistics, supply chains, and military R&D cycles.

Breakout Group 3

Cyber Threat Intelligence (CTI) Sharing Between NATO Allies

Breakout Group 3: Cyber Threat Intelligence (CTI) Sharing Between NATO Allies

- Eman Blair, Senior Vice President for Technology Advancement and Special Advisor, Pentagon Federal Credit Union
- Sally Daultrey, Affiliate, Whole of Government Center of Excellence, William & Mary
- Dr. Andrea Gilli, Lecturer, University of St Andrews
- Roger Yee, Managing Partner, Outcome One

Rapporteur: Alex Bumpers, Student, King's College London

To maintain security in today's multi-domain threat environment, NATO and its allies require strong cyber defence capabilities including effective cyber threat intelligence (CTI) sharing for detecting, preventing and responding to malicious cyber activities. Though a range of NATO cyber defence mechanisms currently exist that share common features among allies, several challenges–not all technical–undermine the effectiveness of CTI sharing among member states and allies. To address these challenges, this breakout group sought cross-sector perspectives on best practices for improving CTI sharing, including insights on how emerging technologies like AI might enhance real-time data exchange and collaborative defence strategies.

Asymmetry and Cyber Threat Intelligence

Asymmetry in capabilities, resources, and supply chains among NATO members and allies challenges how rapidly effective CTI sharing can be achieved. Asymmetry can also be a strength: the best solutions can emerge from less well-resourced organizations in response to crisis, offering learning pathways for all. Joint cyber exercises can be useful for identifying and filling gaps in capability and accountability. Through stress-testing existing or planned cyber defence cooperation strategies, comparative advantages emerge, signalling clear roles and responsibilities that maximize the strengths of individual NATO members and partners.

AI provides both potential benefits and risks for effective CTI sharing. AI models trained on cybersecurity and cyber threat detection knowledge could accelerate education for NATO members with less expertise, by providing a credible knowledge base for learning and

development. However, divergent rates of AI development and adoption in NATO countries may present new forms of asymmetry and potential security risks if models are adopted without sufficient testing, evaluation, experimentation and verification (TEEV). Moreover, NATO countries may be reluctant to share AI-related capabilities due to classification, security concerns, or competition.

Roles and Responsibilities Across Sectors

Participants agreed that public-private partnerships are imperative for effective CTI sharing and for managing innovation in emerging technologies to drive NATO cyber defence. Private CTI firms have global visibility into the cyber threat landscape - beyond that of even the most capable governments - yet the best ideas are not always reflective of the highest competencies: strong CTI culture exists in less well-resourced, smaller groups of trusted actors. Private actors large and small may be better placed to coordinate CTI sharing due to their wider visibility and ability to use informal networks for communication and warning, particularly for more urgent threats.

The group discussed how divergent incentives can undermine effective partnerships between public and private sector. Private actors in particular may be reluctant to share cyber threat information or tools they feel give them a competitive advantage in the marketplace. Effective CTI sharing and delegation of roles and responsibilities requires creative solutions that balance the distinct comparative advantages and incentives of each sector, recognising the value of informal networks and sandboxes to explore ‘what works’.

Threats and the Nature of Cyberspace

Participants considered how the virtual, cross-border nature of cyberspace undermines urgency in sharing CTI. Contrasted with intelligence sharing to counter threats of physical harm, for example in counter-terrorism, CTI sharing requires the balancing of varying priorities and expectations: in the absence of physical threat to life, the architecture of accountability and sharing incentive is more difficult to define. The example of how the United States abides by a “duty to warn” mandate was offered, requiring warning to other nations about known threats to life (this mandate led the U.S. to alert Russia prior to a terrorist attack in Moscow in 2024, showing cooperation even between adversaries). While cyber threats rarely fit the definition of terrorism, the role of informal networks and duty to warn is vital to sharing CTI at time of crisis.

Trust

The group explored the differences between emergent trust that grows slowly over time, and trust that appears in times of emergency. Both forms are critical for effective CTI sharing, but can be undermined by competing objectives, even among allies and partners.

For example, the U.S. temporarily paused intelligence-sharing with Ukraine amid diplomatic tensions in early 2025. NATO members and partners may not trust the security of critical infrastructure or cyber defence systems of allies; many are prioritising adoption of technologies made in-country. The group agreed that understanding risk tolerance is a necessary part of CTI sharing, and the traditional risk-averse stance of governments must transform to facilitate effective CTI sharing.

The Human Factor

Challenges for CTI sharing are often discussed in purely technical terms - for example, misalignment of taxonomies, difficulties in reconciling threat indicators, incompatible architectures. This strong focus on technology overlooks the human challenges around trust and organizational culture that can block - or enable - sharing. Participants discussed how the varying definitions of CTI have emerged, differentiating between cyber threat information and intelligence, agreeing that effective sharing relies on consensus among sharing parties about what gets shared, with whom, with what expectations. Intelligence always has a context: while AI can automate processes to help flag malicious cyber activity, effective CTI sharing will remain driven by human insight to navigate context, distilling intelligence to inform actions.

Takeaways:

- Conduct joint cyber exercises and policy hackathons to clarify roles and responsibilities for CTI sharing across NATO members and partners, strengthen collaborative defence strategies, and identify scenarios that may challenge trust, toward enabling proactive cyber threat mitigation.
- Streamline public-private partnerships for CTI sharing by developing solutions that align divergent incentives between the two sectors to avoid tensions that can undermine trust and cooperation.
- Leverage AI to automate indicator-and-warning processes and support education among less cyber-capable stakeholders while mitigating additional AI-driven asymmetry and security risks which could undermine trust and interoperability.

Outcomes: Identification of best practices for improving cyber threat intelligence sharing with NATO, leveraging AI to enhance real-time data exchange and collaborative defence strategies.

- Providing intelligence without dictating how it should be used.
- Working from a shared understanding of mission and threats builds a culture of collaboration and willingness to contribute intelligence.
- Working from a shared definition of cyber threat intelligence among partners.
- Identifying gaps in CTI sharing processes through joint cyber exercises and hackathons.
- NATO’s malware information sharing platform (MISP) and the Common Vulnerabilities and Exposures (CVE) system have proven highly effective in establishing a common language and taxonomy for threat sharing, offering an architecture for next-generation CTI sharing, toward shared data standards among partners.

- Building towards more robust processes for CTI sharing by starting with ‘what works’, identifying the basic parameters that provision trusted sharing.
- Sharing known cyber defence weaknesses, such as improper storage techniques, as opposed to only information related to urgent threats.
- Ensuring practitioner perspectives are represented in discussions on how to improve CTI sharing.
- Using informal networks for CTI sharing, particularly for more urgent threats where quick communication is critical, recognising their value in a trust architecture that transcends borders and boundaries.