Information & Security

Nadja El Fertasi, vol. 42 (2019): 33-47
https://doi.org/10.11610/isij.4202

Published since 1998 ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Why Digital Ecosystems of Civil-Military Partnerships Are a Game Changer for International Security and Defence

Nadja El Fertasi

NATO HQ, Brussels, Belgium
https://www.ncia.nato.int/

Abstract

The defence and security sectors are grappling to keep up with the rapid changes that the digital transformation is having on societies. By 2030, people will have access to unprecedented volumes of information available through networks across the globe. Enhanced connectivity will expose both civil and military networks to threats at a pace never seen before. Threats and challenges associated with the digital change of Big Data, the Internet of Things or disruptive technologies such as Artificial Intelligence continue to make current headlines. Partnerships between civil and military institutions in the digital era will help mitigate the misuse of technology while fully harnessing its opportunities. As we move into a new era where information and hybrid warfare continue to mark the security landscape, digital ecosystems of civil-military partnerships will prove valuable for the long term. An era where a comprehensive, diverse and an inclusive lens in implementing defence and security policies is a necessity to reflect the complex and interrelated security challenges of today's age. Building on the public-private transatlantic forum, such as the NATO Industrial Advisory Group by tapping into the full potential across the Alliance, will help ensure NATO stays ahead of the technology curve. Bringing public-private partnerships into the digital era to keep pace with the challenges of digital transformation and disruption is no longer a luxury, but a necessity.

Article Info:

Received: 19 Mar 2019
Revised: 20 May 2019
Online: 22 Jun 2019

Keywords:

digital transformation, digital disruption, civil-military relations, NATO, defence and security

✉ E-mail: elfertasi.nadja@gmail.com

Introduction

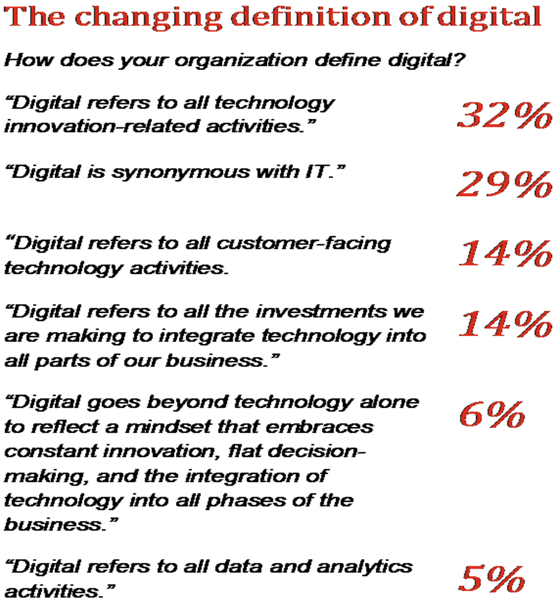
The defence and security sectors are grappling to keep up with the rapid changes that the digital transformation is having on societies. By 2030, people will have access to unprecedented volumes of information available through networks across the globe.[1] Enhanced connectivity will expose both civil and military networks to threats at a pace never seen before. Threats and challenges associated with the digital change of Big Data, the Internet of Things or disruptive technologies such as Artificial Intelligence continues to make current headlines. Partnerships between civil and military bodies in the digital era will help mitigate the misuse of technology while fully harnessing its opportunities.

People at the Heart of Digital Transformation

Before we explore the concept of digital civil-military ecosystems further, understanding the key drivers of digital transformation is of great importance. According to Ferry Abolhassan, digital transformation requires the cloud, trust and should be led as part of any management function from the top.[2] Human behaviour should be at the core of this transformation, yet the importance of human capital remains underestimated.

A recent report published by PwC[3] argues that human interaction and how people experience the digital transformation are at the core of any successful change across the business enterprise. PWC's survey found that by focusing on "Putting people at the heart of transformation" is a phenomenon still in an embryonic phase and needs to be led and driven by the top leadership of any organisation. A strategy that fosters a culture of innovation where people are risk tolerant instead of risk averse; where failing fast and going forward is seen as positive change; and where a safe environment is cultivated so that individual excellence as part of collective creativity thrives, will ultimately lead to agile and resilient organisations equipped to deal with the challenges of the digital era. Human experience across all facets can significantly raise an organisations' 'Digital IQ' (see also Figure 1). As Kane and co-authors state,

> The ability to digitally reimagine the business is determined in large part by a clear digital strategy supported by leaders who foster a culture able to change and invent the new. While these insights are consistent with prior technology evolutions, what is unique to digital transformation is that risk taking is becoming a cultural norm as more digitally advanced companies seek new levels of competitive advantage. Equally important, employees across all age groups want to work for businesses that are deeply committed to digital progress. Company leaders need to bear this in mind in order to attract and retain the best talent.[4]



The changing definition of digital

How does your organization define digital?

"Digital refers to all technology innovation-related activities."	32%
"Digital is synonymous with IT."	29%
"Digital refers to all customer-facing technology activities.	14%
"Digital refers to all the investments we are making to integrate technology into all parts of our business."	14%
"Digital goes beyond technology alone to reflect a mindset that embraces constant innovation, flat decision-making, and the integration of technology into all phases of the business."	6%
"Digital refers to all data and analytics activities."	5%

Figure 1: How we define 'digital.'
Source: PwC 2017 Global Digital IQ Survey.

Digital Transformation for the Military Side of the House

How does this translate into the military side of the house? How do governments and large multinational security institutions adopt and drive digital transformation to ensure they remain ahead of the technology curve? The unexploited potential of the cooperation between public and private sectors only makes societies more insecure, in an era where digital natives are in overflow and often outside of the military sector. Tapping into human potential across the civil-military spectrum by including solutions developed by non-traditional stakeholders has the potential to be a real game changer for the defence and security.

This will require a shift of mindset amongst policymakers to start adopting business principles from corporate and civil society without renouncing the core values of institutional bureaucracy. A high Digital IQ in multinational institutions and governments will reap benefits beyond imagination if we invest in the people and unleash their creative excellence and innovation. An innovation that is needed to bring about constant journey of culture and mindset change in the defence and security sector.

Complex problems require inclusive solutions fuelled by comprehensive and cross-cutting disciplines, as well as rethinking how military doctrine, concepts, and policies can support civil actions and vice versa, in a world where boundaries between civil and military technology threats continue to be blurred. Investing in next-generation capabilities and agile acquisition methods is what will keep institutions like NATO ahead of the technology curve as technology refresh cycles get shorter and shorter.

Digital transformation is a constant effort about transforming technology and changing mindsets to embrace the power of change. Building an ecosystem of partnerships, including industry and academia across the Alliance, is a strategic resource. This article argues that by taking civil-military partnerships into a new era, the security sector will be better equipped to address the challenges of digital transformation while fully embracing its opportunities. This is an era where a comprehensive, diverse and an inclusive lens in implementing defence and security policies is a necessity to understand the overwhelming digital and hybrid security challenges.

Homogenous Partnerships Are Part of the Past

With quagmires popping up across the globe, the conflict spectrum continues to grow. Addressing security challenges and risks/threats through a 360-degree lens, NATO adapts to the ever-changing character of conflict demands new approaches.

The GLOBSEC report on NATO's Adaptation Initiative released late last year,[5] was unapologetic about the threats facing the Alliance from numerous angles, ranging from hybrid to hyper warfare at a pace which continues to evolve faster than anticipated. The current strategic landscape is marked by 21st century information warfare where superiority in the sea, land, air and space is becoming critical, while competing at a level below war where peer-state competitors have successfully integrated information operations, cyber, political influence, economic coercion, and information operations.

Geopolitical Context

Before we dive deeper into the challenges the defence and security face, a brief overview of the geopolitical developments is merited. Since its inception, the Alliance's political-military bureaucratic arm, NATO, has witnessed several phases from the Cold War period to NATO's enlargement with Eastern countries, to post-9/11 era focusing on expeditionary operations and crisis management, to the current era where a new focus on defence and deterrence dominates the security agenda

Russia's annexation of Crimea and the instability emanating from the Southern flank requires balancing between an increased defence and deterrence posture in the East, and at the same time projecting stability in the South. Also, the High North is likely to become a contested area as Russia will see the so-called "Northeast Passage" becoming navigable accessing a wealth of natural resources. Furthermore, implementing the Alliance maritime strategy is increasingly under pressure to protect sea lines of communications in an environment where maritime security is primarily a sovereign activity; yet NATO's maritime posture relies heavily on national contributions that continue to be scarce.

Transatlantic relations have reached another turning point in an era where the international liberal order is under threat across both sides of the Atlantic. Current disruptive foreign and domestic policy dynamics and geopolitical developments are seen by many as a crisis in the international liberal order, threatening the future of multilateralism. Multilateralism has been a crucial foundation underpinning the Alliance for the past 70 years, and which is currently challenged by both state and non-state actors from multiple angles across the globe. Still, it is not all doom and gloom as current darkness provides an opportunity for light to enter through subnational diplomacy. Digital civil-military collaboration provides opportunities for leaders and change agents in civil society to step up and work hand in hand with the military to demonstrate the digital potential the Alliance has to offer. A potential that is critical to unfold in an era where information superiority has become the new arms race.

Digital Ecosystems of Civil-Military Partnerships are no Longer a Luxury, but a Necessity

Working with traditional and non-traditional partners, training military leaders and soldiers to become digitally literate is essential in an era marked by information warfare for superiority, and where data is the new oil and a strategic resource. Numerous actors in the defence and security sector have been arguing for a digital approach in protecting data while fully harnessing its full potential in bringing civil-military partnerships to the next level. During his speech at the NATO Science and Technology Organization conference, NATO's Supreme Allied Commander for Transformation General Denis Mercier argued that homogenous partnerships are part of the past.[6] Traditional and homogeneous partnerships are no longer keeping us safe from the dark side of technology as peer state competitors, and non-state actors tap into cutting-edge technology at low cost posing highly complex challenges to both military and civil infrastructures. Technology has become the world's nervous system making networks across the globe increasingly vulnerable to a vast array of threats. Bringing in experts from a broad spectrum of disciplines and across generations will help develop innovative and sustainable solutions to technology threats in an era where information superiority prevails.

The Case of Public-Private Partnerships in the United States

The United States has understood the value of establishing public-private partnerships with tech giants to address some of the most complex security challenges digital transformation brings. In his speech to Stanford University, former United States Secretary of Defense Ashton Carter emphasized that a strong partnership between military strategists and technologies would establish a strong pact in an era marked by digital transformation. He added:

> The same Internet that enables Wikipedia also allows terrorists to learn how to build a bomb. And the same technologies we use to target cruise missiles

> and jam enemy air defenses can be used against our own forces – and they're now available to the highest bidder.

This is why, he said, the Pentagon must rebuild the bridge between Washington and Silicon Valley. "Renewing our partnership is the only way we can do this right."

Europe's Innovation Culture Slowly on the Rise

Lines are blurring between governments and private sector and it is essential to maintain an open dialogue in addressing challenges and seizing opportunities digital transformation brings. Countries like Denmark understand the importance of maintaining diplomatic relations with tech giants across the globe as their influence is continuing to grow.[7]

Under President Macron, France has announced ambitious policies and initiatives to position France as a leading European tech hub for digital transformation. Through the establishment of recent Joint European Disruptive Initiative (J.E.D.I) together with Germany, France seeks to establish a European version of the U.S. Defense Advanced Research Projects Agency (DARPA).[8] This initiative comes amidst a call for Europe to step up its innovation culture as it is losing the technology race with the United States, China, and Russia. The challenge remains however that Europe is not one country, but different member states with different policies when it comes to technology innovation. Germany for example still has a long way to go in changing their risk-averse culture before they can embrace innovation to its fullest potential.[9] Finally, the United Kingdom established the company NATS which brings civil-military partnerships into a new era by advancing aviation in the digital age.[10] In a time where air breaches keep defying civil-military boundaries to ensure the integrity of airspace security in Europe, these types of partnerships are a notable example of how the civilian and military sector work together in keeping the skies safe.

Strategic Challenges Facing Civil-Military Partnerships in the Digital Era: The Case for NATO

Focusing on specific pressing security issues where technology can help keep societies safe will demonstrate the power of digital ecosystems across the civil-military spectrum. For example, connectivity between deployed forces as NATO's military posture increases on the Eastern flank is crucial to ensure a high readiness state in the age of modern defence and deterrence. Ensuring interoperability at all levels and at the same speed between different national military forces has already proven to be a daunting task. Including non-traditional stakeholders from the civilian sector only adds to this complexity but is critical to ensure we advance at the same pace when deploying multinational forces. The fast pace developments of digital transformation are only growing in importance and are marking major initiatives like the recently announced EU defence force plan, enhancing military mobility and the Alliance's overall increased readiness posture.

Perhaps the major challenge will be to protect data which is at the heart of the digital transformation as the military is bringing operations into the cloud. Even more so and beyond the data protection, harnessing its full potential to ensure a 360-degree situational awareness across the conflict spectrum is vital. In the meantime, cyber resilience continues making headlines and attacks such as WannaCry are just the tip of the iceberg. Information technology resilience beyond cyber, in an end-to-end approach, is critical to maintaining situational awareness and anticipating threats in both the public and the private sector.

In this digital age, governments, business and civil society depend on a resilient network to avoid becoming crippled by the technology threats. If we take the defence side as an example, the loss of network resiliency can have catastrophic consequences when military commanders loose situational awareness in theatre.[11]

The Challenge of Military Adaptation

> *To keep the military edge and prevail in future operations, NATO forces must continually evolve, adapt and innovate and be credible, networked, aware, agile and resilient.*[12]

Under NATO's renewed collective defence posture, there is a greater emphasis on static versus deployable presence. The efforts underway to implement an adapted NATO Command Structure to achieve NATO's level of ambition are grand. However, what is even more daunting is the cultural change needed within a homogeneous culture to embrace non-traditional ways of working. For example, high readiness and deployment of forces within the needed timeframe remain critical issues for years to come. Challenges and gaps in interoperability, cyber, logistics and hybrid warfare which became prevalent during NATO's enhanced and tailored forward presence require comprehensive and inclusive partnerships beyond the military. This requires tapping into the human potential across disciplines and all backgrounds within the civil-military spectrum.

Capability Process Reform to Fit the Digital Era

A recent IBAN report found that it takes an average of sixteen years to develop and deliver capabilities in NATO.[13] The report recognises that bureaucratic processes in a complex and continuous evolving strategic security environment is challenging. For example, approximately sixteen years to deliver technology solutions for the warfighter is keeping the Alliance behind the tech curve. That's why NATO has made some important decisions and progress in reforming these processes, and especially when it comes to technological intensive capabilities and services. NATO recognizes that, in the digital age, technological life cycles are so short they can become obsolete in matters of months rather than years.

NATO already has existing policies and partnerships in working with small and medium size enterprise industries to strengthen the transatlantic defence industrial base. The future however will largely be driven by finding niche technology solutions to complex security issues which are developed by accelerators of start-ups, academia, government and other not-for profit organisations. Adopting a policy on how multinational security institutions or even individual governments will tap into this sector is critical to stay ahead of the technology curve in the digital age.

This reform may seem like another bureaucratic undertaking with a dose of scepticism for real change given the sensitivities surrounding the national defence industries. By focusing on opportunities within the limits of the institutional processes, chances for real progress are more realistic. Because the alternative of it being solely a paper exercise is not an option in an era where information warfare continues to dominate the security landscape.

Information Technology Resilience beyond Cyber

Cyber has been recognized as an operational domain during NATO's Warsaw Summit and the implementation of a three-year roadmap of implementation is ongoing. The challenge NATO likely faces is that there are still many unknowns, lack of common and clear understanding of cyber space which has different meanings for different actors with different purposes. Cyber does not recognise civil-military boundaries and many argue that cyber should be integrated in all aspects of NATO's adaptation work strands. Another challenge NATO faces is the underestimation of information technology resilience beyond cyber, as network protection is critical in a time where NATO's critical capabilities continue to come on line. As stated in a previous publication,

> Imagine that a long-range ballistic missile is launched and targeting NATO's population, territory or forces. NATO Commanders may only have six minutes to make the strategic decision to engage and intercept the incoming missile. Their reliance on the operational information provided through IT networks is total, ensuring the right information at the right time, in the right place.[14]

Despite challenges of sovereignty of an end-to-end network protection approach, practical measures to mitigate severe disruption of both civilian and military infrastructures are paramount. Situational awareness hinges on these infrastructures, and its loss during air and missile defence operations will have catastrophic consequences in an era of heightened airspace violations.

21st Century Information Warfare and Digital Disruption

Continuous real-time situational awareness through a 360 °-degree lens and intelligence sharing will remain critical drivers for the near and long-term future. Not only is NATO faced with the inherent challenges of intelligence sharing among Nations, but also the challenges of preparing for future intelligence that will increasingly focus on the use of open source data and collaborate with non-traditional intelligence communities to ensure this 360 °-situational awareness. Finally, artificial intelligence and autonomous systems will be critical in new generation electronic warfare and are already in extensive use by Russia as well as other near-peer adversaries. This continues to pose a challenge to NATO as it lags behind the technological curve. Also, the United States third offset strategy is far more advanced than those of its Allies causing interoperability challenges for any future joint operation or exercises. A fundamental question for NATO continues to be what role it should play to remain ready, robust, agile and resilient for the digital era and the 21st century information warfare? The recent Brussels Summit Declaration touches upon this question by stating NATO's high-level political commitment in staying ahead of the technological curve.[15]

Institutional Challenges Facing NATO

NATO as an institution continues to face a myriad of challenges trying to adapt to a digital era. NCI Agency's General Manager vision "NATO's Digital Endeavour" goes a long way in articulating these challenges and implementing solutions through a phased approach and help bring NATO amongst the digital natives.[16] Some core issues are still likely to hamper any progress if not addressed.

First, if we look at a multinational security institution consisting of 29 member nations which have different interests and pace of technological innovation, the gap between the USA and its Allies in Europe is still prevalent.[17] Change and progress will happen but is likely to be slower as large and traditional multinational security institutions are not driven by the same business models as corporate organizations in the private sector. Furthermore, digital transformation should be seen as a journey rather than an end state for it to be successfully implemented. Second, adopting an end-to-end approach in any digital endeavour requires partnerships and agreements between public and private sectors as ownership of digital assets are fragmented across the civil-military spectrum. Finally, the private sector, especially small and medium-sized enterprises and start-ups have a lot to offer in developing niche, cutting-edge, disruptive technology. Working with next-generation technology can bring information superiority for the defence sector to another level. Still, large institutions like NATO remain a black box for these industries to work with.

Potential Solutions in Bringing Civil-Military Cooperation into the Digital Era

Now that we have looked at the environment and challenges the security sector faces when taking civil-military cooperation into a new era marked by digital transformation, let's look at the potential in addressing these challenges. The current strategic environment is not all doom and gloom. On the contrary, when we take a step back and observe from a distance, that is when dots are connected and silos are brought down. Several state and non-state actors are perhaps challenging multilateralism, but it does provide an opportunity for transformational leaders across both sides of the Atlantic to step up and bring about a much-needed turnaround in the transatlantic relations. First, seizing the opportunities of the on-going momentum under NATO's reform of its common-funded capability processes is essential. Policymakers recognise the need for agile processes and adopting a full-lifecycle approach for technology-intensive capabilities which require deepening public-private partnerships. Second, multinational cooperation helps the Alliance advance at different speeds in addressing regional security challenges of neighbouring countries or those countries that have similar stakes. However, most importantly, multinational cooperation supported by NATO as an institution will ensure the core principles and interoperability is the same for all. An example at hand is the Framework Nation Concept [18] where several countries led by Germany come together to ensure their force readiness is maintained by working on multinational projects. Although the impact of digital transformation may not be on the top of their agenda, this type of institutionalised cooperation between different member states who have a similar interest will help expand their focus – a focus which can attract civil and military talent across the defence and private sector to keep pace with the digital disruption on the military effectiveness of the Alliance.

By introducing diverse digital ecosystems into the equation of multinational cooperation, these reinvigorated civil-military partnerships can help governments ensure information superiority in the digital age of the 21st Century. Below are possible examples of practical quick wins.

Partnerships among Governments, Prime Contractors and Accelerators for Defence and Security Sector

A strong and diverse industrial base has always been a politically sensitive topic within the Alliance as all nations want to ensure their return on investment into their national defence industries. Changing international bidding procedures to favour accelerators specialized in cutting-edge technology is likely to be a political and legal no-go for now. So, how can multinational security initiatives tap into this next-generation technology innovators? Establishing partnerships between prime contractors and accelerators of start-ups, academia and research and development bodies is one way of tapping into innovation. A major defence industry prime contractor like Thales has tailored programmes in place working with start-ups based in Paris' tech-hub F1 station.[19] These partnerships help the prime contractor to tap into agile and next-generation technology solutions development which their institutions may not adapt at the pace needed. On the other hand, these tech giants can help mentor next generation tech innovators how to work with large multinational security institutions in addressing their problems.

Another example is tapping into start-ups specialized in disruptive technology. If we take artificial intelligence as an example, the globally recognized start-up Spark Cognition led by Amir Husain has already proven its value for the defence and security sector.

Algorithms will now bring artificial intelligence into the Air Force's planning, programming, budgeting, and execution process. According to the Defense Innovation Unit Experimental (DIUx), this step marks the first stage of Project Quantum, an effort to use machine-learning resources to enhance decision-making capabilities among top military leaders.[20]

Artificial Intelligence (AI) has become the new brand for disruptive technology dominating global debates amongst policymakers and tech giants. AI has the potential to be a game-changer in ensuring information superiority for the defence and security sector. Close collaboration between different actors from all sectors and across the Atlantic will not only help reduce the innovation gap between both sides of the equation, but it will also increase shared and mutual understanding of what AI means for the security sector.

Establish a Transatlantic Defence Innovation & Technology Dialogue Forum

Fostering understanding, sharing best practices and lessons learned through dialogue is crucial for keeping pace with digital transformation on both sides of the Atlantic. This forum, focused on digital transformation at large in the defence sector, can help identify problems which need collaborative approaches across the civil-military spectrum. Understanding the problem first from multiple angles will create a vision all stakeholders stand behind. Establishing this dialogue to foster this shared understanding is one of the essential steps for building inclusive public-private partnerships in keeping pace with the challenges of digital disruption.

NATO has excellent resources that take innovation to the next level fit for the defence sector. The NATO Industry Advisory Group [21] is the primary forum that serves as an industry advisory hub for NATO and has a transatlantic focus. Building on this forum and expanding its focus from information technology to technology at large to include all five domains of air, maritime, land, space, and cyber will reinvigorate transatlantic-public private partnerships in the digital age. Focusing on disruptive technology that is driving digital transformation in the current era is a necessity.

However, the dark side of technology does not recognise civil-military boundaries; thus, involving non-traditional actors is crucial. Rethinking military doctrine and civil-military cooperation in the digital age to maintain information superiority is what will provide ultimate security. Forging partnerships within in-house NATO expertise (e.g., Allied Command Transformation, Science and Technology Organization, NATO Communications and Information Agency) with the civil sector to include prime contractors, small and medium enterprise, start-ups, academia and research and development bodies will bring civil-military co-operation into the digital age.

A forum for developing a shared understanding on what disruptive technology means for different member states on both sides of the Atlantic will set the scene for bridging the widening innovation gap. Anderson and Townsend argue that disruptive technologies have different meanings in the United States and Europe.[22] Add to that the innovation gap both across the Atlantic and within Europe between various member states, understanding how digital transformation impacts the different security landscapes and interests are paramount for closing this gap.

A final aspect to consider is to include all institutional stakeholders from legal, finance, military officers – both users and commanders, the full spectrum of the industry from prime contractors to start-ups, and other non-traditional stakeholders. In particular seen from the recent implementation of Europe's GDPR regulation which impacts transatlantic digital cooperation.[23] A frank and open dialogue on moving forward in ensuring Europe's innovation culture does not fall behind in the bigger world scene is warranted. By establishing this dialogue, institutional blindness across the Alliance will diminish, and more focus on finding opportunities within existing bureaucracies will prevail.

Good Governance at the Outset Must Prevail

For civil-military partnerships to thrive in the digital age, good governance principles must be set at the outset. For good governance to succeed, it must be driven from top to bottom into institutional granularity. There is much to learn from the private sector in adopting principles for programmatic approaches with clear roles and responsibilities, an overview of available funding mechanisms, empowered and accountable individuals, and continued cross-cutting dialogue and reporting to ensure that transparency prevails at all times. For only then can trust be built, a trust which is the foundation for any partnerships. Another essential and perhaps even more important than trust is a shared vision and approach in solving problems through innovation in a world where disruption becomes status-quo. As General McChrystal stated,

> Whether in business or in war, the ability to react quickly and adapt is critical, and it's becoming even more so as technology and disruptive forces increase the pace of change. That requires new ways to communicate and work together. In today's world, creativity is a collaboration endeavor. Innovation is a team effort.[24]

A significant issue, however, remains the much-needed cultural change in defence and security sector to embrace new ways of working. Although we have moved into a new era where complex and interrelated security challenges affect societies across the globe at the speed of lightning, the culture of Cold War is still present in many of the institutions; a culture that is the DNA of the Alliance but no longer sufficient in keeping pace with the challenges and threats in the digital age. Recognizing that this culture is still present is a first step in bringing down barriers. Establishing forums for dialogues and partnerships to flourish is the second step. The third step is to nurture, develop and sustain these partnerships through good governance at the outset of any collaboration – good governance based on a shared vision in addressing pressing security challenges as a result of digital transformation and disruption.

Conclusions

This article attempts to argue the untapped potential of public-private partnerships for the defence sector in keeping pace with the challenges of digital transformation. Digital transformation impacts all strata of society across the civil-military spectrum. In fact, the blurring lines between civil and military roles and responsibilities in the digital age continue to grow. At the same time, the geopolitical context is marked with transatlantic turmoil across both sides of the Atlantic. The future of multilateralism is at stake as both state and non-state actors are challenging the international liberal order. Still, it is not all doom and gloom.

As we move into a new era where information and hybrid warfare prevail, digital ecosystems of civil-military partnerships will prove valuable for the long term. Building on the public-private transatlantic forum such as the NATO Industrial Advisory Group (to include participation of start-ups, academia, not-for-profit organisations and other non-governmental bodies) by tapping into the full potential across the Alliance will help ensure NATO stays ahead of the technology curve. Bringing public-private partnerships into the digital era to keep pace with the challenges of digital transformation and disruption is no longer a luxury, but a necessity.

References

[1] World Economic Forum, "Digital Transformation Initiative," Executive Summary, 2017.

[2] Ferri Abolhassan, ed., *The Drivers of Digital Transformation, Why There's No Way Around the Cloud* (Cham, Switzerland: Springer, 2017), 1-10.

[3] PwC, "A Decade of Digital – Keeping Pace with Transformation," 2017 Global Digital IQ Survey: 10th anniversary edition, 2017.

[4] Gerald Kane, Doug Palmer, Anh Nguyen Phillips, David Kiron, and Natasha Buckley, "Strategy, not Technology, Drives Digital Transformation," *MIT Sloan Management Review*, July 14, 2017, accessed June 25, 2018, https://sloanreview.mit.edu/projects/strategy-drives-digital-transformation/.

[5] John R.Allen, Giampaolo di Paola, Wolf Langheld, Julian Lindley-French, Tomáš Valášek, and Alexander Vershbow, "One Alliance: The Future Tasks of the Adapted Alliance," *GLOBSEC Ideas Shaping the World*, November 27, 2017, accessed June 24, 2018, www.globsec.org/publications/one-alliance-future-tasks-adapted-alliance/.

[6] Denis Mercier, "How will artificial intelligence and disruptive technologies transform military operations and organizations?" NATO Science and Technology Organisation conference, Bordeaux, May 31, 2018, Accessed Jun 24, 2018, www.act.nato.int/images/stories/media/speeches/180531_sto.pdf.

[7] Ministry of Foreign Affairs, Denmark, "About TechPlomacy," Office of Denmark's Tech Ambassador, Accessed June 25, 2018, http://techamb.um.dk/en/techplomacy/.

[8] Daniela Vincenti, "Return of the JEDI: European Disruptive Technology Initiative Ready to Launch," *Euroactiv,* March 16, 2018, accessed June 25, 2018, https://www.euractiv.com/section/economy-jobs/news/return-of-the-jedi-european-disruptive-technology-initiative-ready-to-launch/.

[9] Sintia Radu, "Old Europe vs. New Tech," *US News*, April 5, 2018, Accessed June 25, 2018, https://www.usnews.com/news/best-countries/articles/2018-04-05/the-german-approach-to-tech-investment.

[10] NATS, accessed June 20, 2018, https://www.nats.aero/.

[11] Nadja El Fertasi and Nadja De Vivo, "Resilient for How Long? Information Technology Warfare in the 21st century: The Alliance's Invisible Threat," *Vox Collegii Magazine* 13 (July 2016): 8-15.

[12] NATO, "Framework for Future Alliance Operations: 2018 Report," SACEUR, SACT, accessed June 20, 2018, http://www.act.nato.int/images/stories/media/doc library/180514_ffao18.pdf.

[13] International Board of Auditors for NATO, "Performance Audit Report to Council on the Need to Improve NATO's Capability Package Process," *nato.int*, February 01, 2017, accessed June 20, 2018, https://www.nato.int/issues/iban/perfor mance_audits/170201-improve-capability-package-process-eng.pdf.

[14] El Fertasi and DeVivo, "Resilient for How Long?" p. 8.

[15] "Brussels Summit Declaration," NATO, July 11, 2018, accessed July 12, 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.

[16] Robert K. Ackerman, "NATO Treads Carefully Toward a Digital Future," *Signal*, April 1, 2018, accessed June 20, 2018, https://www.afcea.org/content/nato-treads-carefully-toward-digital-future.

[17] Wendy R. Anderson and Jim Townsend, "As AI Begins to Reshape Defense, Here's How Europe Can Keep up," *Defense One*, May 18, 2018, accessed June 20, 2018, https://www.defenseone.com/ideas/2018/05/ai-begins-reshape-defense-heres-how-europe-can-keep/148318.

[18] Rainer L. Glatz and Martin Zapfe, "Ambitious Framework Nation: Germany in NATO," German Institute for International and Security Affairs, September 2017, accessed June 21, 2018, https://www.swp-berlin.org/fileadmin/contents/products/comments/2017C35_glt_zapfe.pdf.

[19] "Thales has welcomed 9 startups within its Cyber@Station F programme," *THALES,* November 10, 2017, accessed June 20, 2018, https://www.thalesgroup.com/en/worldwide/security/press-release/thales-has-welcomed-9-startups-within-its-cyberstation-f-programme.

[20] Katherine Owens, "AI will now have input in Air Force decision-making," *Defense Systems*, September 05, 2017, accessed June 20, 2018, https://defensesystems.com/articles/2017/09/05/ai-air-force.aspx.

[21] NATO Industrial Advisory Group, "Chairman & Vice-Chairman's Corner," accessed June 20, 2018, https://diweb.hq.nato.int/niag/Pages_Anonymous/Default.aspx.

[22] Anderson and Townsend "As AI Begins to Reshape Defense."

[23] Susan Ness and Peter Chase, "How GDPR Could Affect the Transatlantic Relationship," *GMF Strengthening Transatlantic Cooperation*, May 11, 2018, accessed July 17, 2018, www.gmfus.org/blog/2018/05/11/how-gdpr-could-affect-transatlantic-relationship.

[24] Stanley McChrystal, Tantum Collins, David Silverman, and Chris Fussel, *Team of Teams: New Rules of Engagement for a Complex World* (New York: Penguin Press, 2015).

About the Author

Nadja **El Fertasi** has a drive for building trust and understanding between stakeholders across governments, business and tech sectors to keep pace with digital transformation. She has built a career path in NATO over the past seventeen years taking on a variety of posts in different fields within large multinational NATO institutions. She is also passionate about bridging the generational diversity gap and fostering inclusiveness between different stakeholders in the defence and security sector. Nadja is fluent in Dutch, English, French and Arabic, and is proficient in Italian and German. She is a 2018 German Marshall Fund Marshall Memorial Fellow and a steering committee member of the "Women in International Security Brussels." She holds a Master's degree in International relations from the University of Cambridge and is an alumna of the NATO-wide Executive Development Program.
https://orcid.org/0000-0002-9490-1656
https://www.linkedin.com/in/nadja-el-fertasi-86009320/