# Innovation DA

## 1NC

### 1NC – DA

#### NATO’s “Smart Defense” policy for cybersecurity creates policy resilience to hybrid threats---solves the case while preserving e-innovation

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

Resilience as methodology: NATO’s strategic aim

Resilience is a method. A dedication to the goal. It is therefore an aim. Terminologically is announced in security-led strategies yet also business-led strategies. It holds a completely sound operational aim. To deliver and stick to the requested. It is brand name that defines strategy through which it results to operational capacity that sustains and grows; at the level of NATO, with the capacity to apply in diverse fields of operations adding value, to an already robust policy decision and operational capacity building and actions; at the level of cyber-security policy

resilience to the framework is a “strong-hold” policy to deliver a protection mechanism and method.

Resilience’s framework acknowledges the will for preparedness so as to counter a possible integrative part of possible emerging crises. It is seen as an innovative strategic management policy procedure and tool. Strategically, it applies to operational capacity building, both civil and military. It is an element of acknowledged standardization of procedures. In the defense sector, when forces are deployed, they need flexible and effective means of countering threats; while in the field of cyber-security, they need agility in operational network centric operations, and constant accurate flow of information.

Strategic resilience in cyber-security requires flexible adaptability to new challenges. Its strategic resilience works as a tool for closeness, mitigation, and/or negotiation; it allows for cooperation among allies or members.

NATO’s vigilance and resilience in security-led affairs including cyber-security defines strategic plans and re-assesses risks that will allow us to think entrepreneurial and innovative. For NATO members, Heads of State, and Governments, cyber-security creates a modern administrative and operational format and framework of the alliance at a virtual level that is flexible and e-oriented, reflective to the market needs for security and stability, while augmenting market e-innovation and while adapting to new affordable methods of economic and socio-economic growth. NATO acquires protection mechanisms while its operations and memberships enlarge while operational challenges are upgraded and updated. NATO needs to provide militarily and technologically agile and interoperable forces with added value, through civilian capabilities (NATO’s Cyber-Defense Policy, 2011).

Resilience in security-led affairs through innovation and entrepreneurship therefore should be a leveled adaptation process for NATO; a phase to consequently strategize and draw new scenarios for cyber-security among others. This comes through operational result processes of training and experiences, when countered in an effective manner with lessons to be learned constantly in adaptable new circumstances against any forms of cyber-attacks.

Resilience becomes thus a policy orientation for NATO’s “Smart Defense” clause. NATO boosts on military innovation and methods of operational support and deliverables and protection mechanisms, while remaining relevant as a political military organization, a regional and global asset value to security and strategy application at a time of vast changes and challenges.

#### The plan undermines our tech edge

Camille Grand 20, NATO’s Assistant Secretary General for Defence Investment, Matthew Gillis, Defence Investment Staff Officer at NATO HQ, "Alliance capabilities at 70: achieving agility for an uncertain future", NDC Policy Brief No. 01, Jan 2020, <http://www.ndc.nato.int/news/news.php?icode=1408>

Secondly, the pace of change has accelerated at a tempo that risks outpacing our ability to exploit and, as necessary, counter the technological advancements on the horizon. Many of these technologies are driving towards faster and more distributed decision-making, which in turn bumps up against the sometimes bureaucratic and conservative nature of NATO’s machinery and decision making. Posturing the Alliance to fully embrace these technologies will require an adapted mindset and culture of delegating authority and accepting ambiguity.

One case for improvement is in the area of NATO processes, particularly those that manage procurements, standardization, and capability life cycles. We often strive for perfection in our future requirements, and engineer our processes around numerous decision gates and complicated management structures. The result is a capability that can be over budget, late, and obsolete when delivered. NATO has taken some healthy steps in this direction with the adoption of a new model for governing common funded capabilities with fewer decisions and streamlined oversight. But continued efforts are needed.

Industry also has a substantial role to play in this area. Our traditional defence industrial base should not be complacent with a business model that can be slow, cumbersome, and risk averse. In what Klaus Schwab has defined as the “fourth Industrial Revolution”, the changes on the horizon “herald the transformation of entire systems of production, management, and governance”1 while entirely upending existing industrial value chains. The success of Allies’ industries will depend on more acceptance of risk, greater investment in research and development, and an adapted mindset towards partnering with players outside the traditional defence sphere.

#### The impact is great power war

Jim Talent et al 19, Senior Fellow, Bipartisan Policy Center, Former U.S. Senator (R-MO), Robert O. Work, Distinguished Senior Fellow, Center for a New American Security, Former Deputy Secretary of Defense, 12/3/19, "The Contest for Innovation: Strengthening America’s National Security Innovation Base in an Era of Strategic Competition", Report of the Task Force on 21st-Century National Security Technology and Workforce, The Ronald Reagan Institute, https://www.reaganfoundation.org/media/355297/the\_contest\_for\_innovation\_report.pdf

The United States has entered an era of long-term competition with revisionist powers. A key aspect of this competition will revolve around a contest for technological superiority waged between the national innovation bases of the respective competitors. The outcome of this competition will determine not just American national security but also how the nations of the world interact—and whether a free and open political and economic system will remain the foundation of those interactions.

After a long post-Cold War focus on rogue regional powers and nearly two decades of continuous warfare in the Middle East and a focus on rogue regional powers, the United States now faces a new defining national security challenge: a long-term strategic competition with a resurgent Russia and a rising China.

Russia seeks to reestablish itself as a global power. While Russia is able to compete with the United States militarily in certain domains, its economic outlook and long-term demographic prospects are grim. Accordingly, it is unlikely to develop and nurture a true national innovation ecosystem. Given these disadvantages, Russia is limited to acting as a geostrategic spoiler seeking to undermine and weaken the United States, its alliances, and its global interests.

China, on the other hand, is already challenging the United States economically, militarily, and politically. China’s economy has surpassed that of the United States in terms of purchasing power parity and could, under some scenarios, pass the U.S. GDP in absolute terms in the mid- to late 2020s. Under the leadership of the Chinese Communist Party, China defines its vital national interests in ways that are irreconcilable with both the interests of the United States and the values of self-determination and individual freedom to which we and our allies are committed. China’s global expansion, from both a trade and military perspective, is challenging the United States in virtually every region of the world.

In pursuit of its goal of reshaping the world order, China aims to supplant the United States as the world’s leading technological power by 2030. China has articulated a distinct strategy of statedriven innovation, defined by its concept of “military–civil fusion,” to lead the world in cutting-edge technologies that might allow it to leapfrog the United States both economically and militarily.

That strategy presents a two-fold challenge for the United States. Economically, the challenge is to sustain American prosperity and access to markets on equal terms with other nations against China’s ambition to control the economic sectors that will determine national primacy in the decades ahead.

Militarily, the fundamental mission of the U.S. government (USG) is to deter a great-power war and, if deterrence fails, to prevent escalation of the conflict and end the war on terms favorable to the United States and its allies. An important key to this mission is achieving and maintaining military–technical superiority. However, over the last several decades, China—and, to a lesser extent, Russia—has invested heavily in advanced military capabilities specifically aimed at overcoming the technological lead of America’s armed forces.

As a result, the conventional overmatch that the United States has relied upon to undergird its deterrence posture since the end of the Cold War is eroding. The balance of power in East Asia has already shifted substantially in China’s direction. If this trend continues, effective deterrence in that region will likely fail, leaving the United States to face the unattractive alternatives of accepting aggression against its interests or its allies or triggering armed conflict with the People’s Liberation Army (PLA), with all the attendant risks of escalation.

## 2NC

### Overview---2NC

#### Tech dominance is key to winning great power wars—the foundation of military strength is economic strength---there’s a huge first adopter advantage for emerging tech that will determine who wins the wars of the future

#### The DA accesses a better internal link to tech innovation than the aff---NATO needs a tech innovation pipeline that can provide more defense at less cost with least delay---but that requires an agile bureaucracy willing to make big bets to incentivize the creation of entirely new markets of defense tech---an Alliance wide approach is better than a fragmented uncertain strategy

#### Framing issue---maximize innovation---the more the better---we don’t have to win the aff ends all innovation---just that they erode the pace, scope, and coordination of developments

#### Tech dominance is key to future wars---hypersonics, biotech, and AI

Charles Lutes 19, director of the Office of Defense Coordination at Lawrence Livermore National Laboratory, previously the director of the Center for the Study of Weapons of Mass Destruction at the National Defense University in Washington, D.C., currently pursuing a Ph.D. in Public Policy from The George Washington University, “U.S. Defense Strategy and the Innovation Imperative”, Getting Innovation Right, Center for Global Security Research, Lawrence Livermore National Laboratory, Sept 2019, https://www.osti.gov/servlets/purl/1635772

The point of departure for any contemporary analysis of the means and ends of innovation for national security should be the 2018 National Defense Strategy (NDS).1 The strategy describes a complex and dynamic security environment marked primarily by a renewal of rivalry among the major powers and with it new forms of strategic competition and new forms of strategic conflict. Among the dynamic elements it highlights is the technological dimension: strategic competition with Russia and China is characterized by a seemingly relentless drive to develop new technologies— advanced computing, big data analytics, artificial intelligence, autonomy, directed energy, hypersonics, and biotechnology. Multiple simultaneous technological revolutions are likely to significantly impact the character of war. The competitor that best harnesses these technologies will have the advantage in fighting and winning the wars of the future. The NDS exhorts the nation to foster a competitive mindset and emphasizes the need to “out-think, out-maneuver, out-partner, and out-innovate” our competitors and potential adversaries.

It is not surprising that the NDS focuses on innovation as a key to out-competing adversaries during a period of rapid technological change. At the same time, the NDS hints that technological innovation is a necessary, but not sufficient condition, for outinnovating the competition. As technology advances, the nation’s military must also seek to innovate its operational concepts and doctrine, as well as its organizations. Each is explored below.

#### Coordinating tech innovation solves all global challenges---saves humanity

Daniel **Araya 20**, PhD, Public Policy, University of Illinois at Urbana-Champaign, Senior Partner with the World Legal Summit and Senior Fellow with the Centre for International Governance Innovation, 9/1/20, "Is The Venus Project The Next Stage In Human Evolution?", Forbes, https://www.forbes.com/sites/danielaraya/2020/09/01/is-the-venus-project-the-next-stage-in-human-evolution/#1d09e43c5c35

A seismic shift is under way. Against the backdrop of rising temperatures, collapsing ecosystems, and the threat of species extinction, technologies like artificial intelligence (AI) and robotics are now moving to transform the global order. Indeed, for the first time in our history, we have the tools and technologies to guide and shape our evolution. But what will this future look like?

I recently spoke with Roxanne Meadows and Nathanael Dinwiddie of The Venus Project to better understand their thoughts on the future. As they explain, the status quo is no longer working. Climate change, social inequality, and technological innovation are now disrupting a market-driven society. The key to resolving these global challenges, they suggest, is rooted in a Resource Based Economy.

The term “Resource Based Economy” was first coined by Jacque Fresco, the founder of The Venus Project. Fresco believed that a Resource Based Economy could support the scientific integration of automating technologies (AI and robotics) and engineering systems in providing the highest possible living standards. Meadows and Dinwiddie suggest that this kind of economy is the next stage in human evolution. But what do they mean?

1. What is The Venus Project?

Meadows and Dinwiddie: The Venus Project is a non-profit organization that presents a new socio-economic model utilizing science and technology. For the past 40 years, we have maintained a 21-acre research center in Venus, Florida. We propose a new scientific foundation in transcending humanity’s current problems by testing a new social design for organizing our society as a global “operating system”.

Taken as a whole, the Venus Project fills the egregious gap between the sciences and the humanities by combining a social philosophy of the future with technical knowledge applied at a global scale to solve the problems of the human condition. Our methodologies are designed to realize the full potential of science and technology to achieve social betterment for all living systems— without exception. Our approach to social organization calls for changes in governance, economics, urban planning, education, human relationships, language, and values.

2. We appear to be in the early stages of a massive economic depression. What is your sense of what is happening politically and economically right now?

Meadows and Dinwiddie: We are witnessing an unprecedented political polarization and economic disruption around the world today. The status quo is no longer working. Many people are now beginning to understand how dysfunctional the management of nations, peoples, and resources has been. Human needs and the needs of our environment are far too complex to be managed by political means, arbitrary economic direction, or an elite without the relevant understanding of science and technology.

Compounding this problem, nature operates as a closed-loop system, but we do not. We extract resources without replenishing them, accumulate waste materials without recycling them, and we pollute our air, water, and food crops for the need to maintain competitive profit margins. There are many other factors converging at once besides the pandemic, all of which contribute to the system’s unrest.

3. Younger generations seem disaffected with Capitalism. Could you describe your vision of a post-scarcity society?

Meadows and Dinwiddie: The Venus Project recognizes that if we utilize a global systems approach as a basis for organizing and managing resources, we can design a much more humane environment for all. Our goal is to advance the health and the protection of the ecosystem, as opposed to the accumulation of wealth, property, and power. We do not have enough money to fulfill the needs of the world’s people, but we do have enough resources, if wisely managed. Ultimately, it is not money that people need, but unencumbered access to the necessities of life and self actualization.

Accomplishing this is a technical and engineering challenge requiring massive coordination by transdisciplinary teams of engineers and scientists in managing the Earth’s resources within its carrying capacity. This kind of scientific endeavor would eliminate the vicious rivalries over scarce resources and, in turn, generate very different behavior amongst people.

Briefly, this is what Jacque Fresco, founder of The Venus Project, termed a “Resource Based Economy”. This is a necessary step for humanity’s evolution. It could be thought of as a new science, a science of Earth Management where, by necessity, all of Earth’s resources become the common heritage of all the world’s people.

4. How does the Venus Project differ from Socialism or Communism?

Meadows and Dinwiddie: Rather than worker revolts and the forcible overthrow of the system (Communism), or the redistribution of capital (Socialism), The Venus Project approaches social change as a process of guided evolution. In our view, the challenges before us are a matter of engineering and design. The Venus Project calls for an experimental analysis of a new social system. This system is unlike any communist revolution, utopian commune, or coup d’état tried in the past.

In our view, the fundamental issue limiting social management in the past has been the lack of an effective data-driven methodology for evaluating and improving the system’s functioning. Full-scale blanket application of social policies to vast geographic areas— be it through revolution or legislation— without a means for evaluating their effectiveness, follows from an approach heavy in ideology but short in scientific method. The Venus Project calls for iterative prototyping of cities that we take as the unit of analysis in validating or falsifying hypotheses. All of this begins with testing a prototype, not a revolution.

Although Karl Marx did envision a society wherein money, private property, and social hierarchy were abolished, he could not begin to imagine how to implement this system at a technical level. In contrast to Communism, The Venus Project calls for the total redesign of cities (transportation, distribution, manufacturing, recycling, infrastructure) to produce abundance of goods and services. This is achieved through automation and optimized infrastructural efficiency.

5. What role does technology and automation play in The Venus Project?

Meadows and Dinwiddie: For the first time in history, we have the tools and technology to guide and shape our evolution. To accomplish this, The Venus Project advocates the humane and intelligent use of technology and the methods of science directed toward the well-being of all people and the environment which sustains all life.

In our view, technology and automation should be strictly used for social betterment and to eliminate repetitive, dangerous and monotonous work. If automation displaces a job, for example, that means all people would gain more access to the products those machines produce. The necessities of life are distributed without a fee with the aim of expanding to all goods and services. Consequently, there is no threat resulting from technological labor displacement. On the contrary, technology and automation have the potential for enhancing the world’s standard of living, enabling people to learn, spend time with their families, travel, and confront the new frontier of challenges in improving the resilience of the system as a whole.

6. How do you envision utilizing AI in decision-making?

Meadows and Dinwiddie: Applying the methods of science and technology (including AI) to the operation of the world’s societies will lead to a substantially more reliable functioning of support systems than we have today. Homelessness, starvation, war, and environmental degradation are consequences of today’s political and economic approaches to decision-making. A Resource Based Economy operates within a unified systems approach that utilizes the methods of science and AI to arrive at the most appropriate decisions at any given time. Unlike today’s implementation of technology, this new approach would be carefully carried out with the utmost human and environmental concern. The real-time influx of quantitative and qualitative data would provide real-time feedback, enabling humanity to constantly observe and continually improve the operation of the system over time.

7. What are the future goals of The Venus Project?

Meadows and Dinwiddie: At present, we are focused on formalizing and systematizing the body of work of The Venus Project’s founder, Jacque Fresco. In an age that is sorely lacking an approach updated to current knowledge and capability, we enter uncharted territory with the methods of science to help us through. This is the crucial job that no one has attempted, until now.

In the short term, we are focused on a systems approach to organize a holistic understanding of the natural world and human culture. This involves understanding economics and human social systems in the broader contexts of Earth processes and ecosystems, and communicating this understanding through books, videos, the internet, podcasts, transmedia storytelling, and course curricula.

In the mid-term, we aim to fulfill the desperate need for the strategic coordination of consilience by synthesizing the knowledge of academia and the know-how of industry. This network of intelligence will produce a transdisciplinary research agenda, research program, and global theory of change. Constructing a new planning center will function as a living lab and think tank devoted to designing the first prototype city.

In the long term, The Venus Project hopes to see the construction of new prototype cities for the purpose of testing the hypothesis of a holistic, technical design-solution for a social system. Iterations of these prototypes will form a worldwide network of cities. The study of these cities will function as the basis for a science of Earth management, the models of which guide the intelligent allocation of resources for the purpose of optimizing civilization to adapt and evolve in relationship with an Earth ecology.

There is a lot to consider and we welcome participation in the development of such a system.

### Overview---Turns Case---NATO/Russia

#### Innovation provides the adaptability NAO needs to meet future strategic challenges

Julian Lindley-French 20, Senior Fellow at the Institute for Statecraft in London, ““NATO@70”: still adapting after all these years”, NATO at 70: No Time to Retire, NDC Research Paper, NATO Defense College, No. 08, Jan 2020, http://www.ndc.nato.int/news/news.php?icode=1414

Future adaption: what are the most likely evolutions of the Alliance looking forward?

The complexity of NATO’s future adaptation challenge must not be under-estimated. The modernisation of Russia’s armed forces is part of a new form of complex strategic coercion that employs systematic pressure across 5Ds of disinformation, destabilisation, disruption, deception and implied destruction. Moscow’s enduring aim is to use the implicit threat of force to keep the Western allies permanently strategically, politically and militarily off-balance and the threat of overwhelming force as a form of strategic extortion racket focused on those at the margins of the Alliance. As a consequence, future adaptation and the Alliance concept of deterrence and defence will require an entirely new and innovative concept of protection and projection.

The nature of future war must also be seen within the context of the emerging complex strategic coercion that Russia is pioneering. Technology-led cross-domain warfare will see the battlespace become an integrated air, sea, land, space, cyber, information (including electronic warfare) and knowledge super-domain for the conduct of operations. Faced with such threats transatlantic political cohesion and Alliance military interoperability will be vital. The Alliance and its member states must be in the vanguard of the Revolution in Military Technology that is now underway. Artificial intelligence, quantum computing and machine-learning, nano-technologies, drone and other semi or fully autonomous delivery systems are now appearing in a battlespace that stretches from the depths of the oceans to outer-space, across all landmasses, and within and between changing societies and communities.

Adapting NATO to meet the strategic challenges of the twenty-first century must thus be the priority for “NATO@70”. If not, there is a very real danger the Alliance will lack the nimbleness to meet strategic change and technological developments, and ultimately fail as a consequence. There is also a danger that Alliance cohesion will progressively fade if such ambitions are not properly enunciated through a new Strategic Concept that enshrines at its heart a new form of flexible response. Above all, European words must be matched by European deeds through further organisational and internal reform to enable a properly agile and modernised Alliance that would give meaning to the 360-degree approach and enable the Allies to strike a balance between technology, capability and affordability

### Overview---Turns Case---Hybrid Threats

#### Smart defense solves hybrid threats

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

NATO cyber-security policy should never stop transforming, while technology progresses and threats expand to a new and deeply digitized world of insecurity starting with the case with the cyber-attacks in Estonia in 2007 (Rehman, 2013). Past events in Estonia showed early on a strong smart cyber-defense “umbrella” which is certainly still needed by 2018, in which agility and resilience needs to be achieved.

There is a need of a resilient cyber-security strategic policy, a methodological and operational approach for a continuously standardized practical operational preparedness so as to constantly be able to counter cyber-attacks of hybrid or non-hybrid nature. Innovative methodology and ideologies are needed to process such a policy approach. There is a need for clear innovation and entrepreneurial understanding of what constitutes cooperation in cyber-security efficiency knowledge acquiring information and cooperation between public-private institutions and agencies.

A strategic cyber-security policy when applied will allow for the 30 member states to counter with more agile ways any emerging crises. This will efficiently manage processes and purposes for operations against any methods of electronic warfare. Interoperability of forces for joint use in cyber-defense is expected to be achieved through an adaptability and standardization process period. NATO should “e-volve” as should Alliance “e-networked” States. NATO should innovate and manage. NATO should administer change on methods of smart resilience in defense through cyber-security policy, strategically and operationally.

#### Agility and adaptability are key

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

Operationally, national and cooperative forces need to be continuously agile and technologically advanced. In an asymmetrical world, which is complete with unforeseen challenges and threats, we need forces with flexibility, adaptability, operational and strategic command structure, based on high technologically sophisticated information “coming in,” but also being used while in training or through active operations.

On a theoretical scale, the current article requests a cyber-security strategic framework adoption of resilient adaptability and interoperability policy in the framework of safety and defense. The article considers that understanding the realities of threats is by definition a natural innovation and as we move ahead, we structure and operate a single strategy on cyber-security against a virtual threat from wherever it comes from. Its long-term resilience may be more complex as operational capacity needs to constantly develop and adapt into the convergence of societal structures, and methods; where socio-economic, technological, defense even health, and education issues are affected.

When theory on cyber-security, resilience, and operational capacity will be applied at NATOs level, it will enable allies and members, jointly, to create a true policy and strategy for cyber-security resilience against hybrid virtual threats. The methodology on how to is presented through this current article.

### UQ---Smart Defense---2NC Solves Case

#### The DA is a status quo gradualism counterplan with an external impact of tech dominance

#### Smart Defense solves the case now---it’s a defense posture to hybrid threats that uses bottom-up, business-led input to determine how we should respond---but broad Article 5 interpretation is key---it incentivizes tech innovation in order to stay prepared against all hybrid threats

#### Smart Defense solves clarifies NATO’s response to hybrid threats---avoids over and under reactions

Marios **Efthymiopoulos 19**, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

Associating smart defense with cyber-resilience: “engagement through policy adaptation”

As fiscal austerity measures are applied and cutbacks are in effect, according to the Chicago Council on Global Affairs, NATO allies have to decide on methods to approach NATOs political agenda decisions. Allies must enhance capacities and capabilities to implement new and innovative methods of tactical management for the benefit of security toward the Alliance space (Chicago Council on Global Affairs, 2012). According to the Atlantic Council, “…The Alliance, given its new strategic landscape, currently finds itself in, requires a new strategy. NATO’s current three core tasks—collective defense, crisis management, and cooperative security—are ‘tasks’ but not strategies—they do not identity the full spectrum of ends, ways, and means, and therefore do not tell the Alliance and its members either what to do or the risks involved. NATO has been working diligently but without great clarity or common agreement as to its end goals (NATO’s Cyber-Defense Policy, 2011)”.

Heads of States and Governments do listen and observe, but are not keen in stepping in the extra mile; to therefore consult and call on NATO to hold Summit meetings, to negotiate or mitigate current issues, and to elaborate and concentrate more on economic, political, military and management innovation and efficiency of administrative cooperation in all policy regulated fields of NATO.

A strategic framework policy on “Smart Defense,” which is yet to be achieved by 2020, may render a cheaper cost for the total sharing of burden by member states, while attracting more elements or variables where technology can be used to minimize costs. Surely, not all members share the same burden to this day by are reflective to all countries security defenses when it comes to cyberspace.

While a policy on smart defense lowers overall long-term cost, and if burden sharing is actually increased but equaled to lower levels of fiscal sharing, long-term results will show, that in fact, less cost will be achieved and cyber-innovative methods can help mitigate possible costs.

While cyber-security becomes a core, NATO policy for smart defense and resilience attracts attention to stake holders. Through evolving and constant communication and marketing perspectives, social media and workshops, and conferences, cyber-defense should continue to be promoted and have a clear aim. Reflecting on the needs for a global element of cyber-security against current and emerging challenges, exchange of scientific information and operational processes promote such ideology, where experts from around the world exchange information and discuss the risk assessments and how to manage.

Cyber-security then works as a “decree of specialization, which now requires adaptation if not done so already for each member state”, politically, strategically, tactically, and operationally but also legally. Cyber-security must and should always be provided as a methodological tool for operational success of NATO against current and emerging threats. It is and will always be a tool for a joint framework of cooperation, globally.

As smart defense is being upgraded and developed, cyber-defense “…not a conception but a real-politic issue… (Efthymiopoulos, 2008b)”, should remain an element of specialization policy, a key for concrete strategic engagement of all resilient member states. It will emerge to become a policy of innovative unity among states (political) yet also business continuity (strategic orientation) about the future of NATO (The entrepreneurial and managerial side of things).

NATO’s strategic approach post Warsaw and Brussels of 2017 and 2018 Summits is estimated to reflect a much need realistic plan of operations and engagement in the field of cyber-security and defense. NATO should continue to be collective to be a force projector and force protector. It should not limit its role and actions but should allow and seek out enlarged cooperations tailored to the global and regional needs to counter the existing challenges or emerging challenges, considering that as aforementioned challenges are now borderless.

Cyber-security and technological progress within NATO are synonymous. They can therefore be seen as the core of collaboration on smart defense, to be finalized and achieved by 2020 standards. Cyber-security being technologically advanced is resilient to changes and is innovative as a method as it was never been done before at NATO until the date that it was presented to. It does provide adaptable technological architecture and posture, which will be discussed below considering the opportunities but also challenges. It will provide robust deliverables with minimum human capital, fiscal but requests technical deliverables.

### UQ---Smart Defense---AT: UQ Overwhelms

**It's going to be finalized this year---but the aff undermines efficiencies by creating gaps in coverage**

Marios **Efthymiopoulos 19**, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

By 2008, seven Alliance countries according to the Memorandum of Understanding on the cyber-defense center, supported Estonia to get full operational capability (Germany, Italy, Latvia, Lithuania, Slovakia, and Spain), which lead to an evolution period. By 2016, NATO Allies are expected to discuss further and finalize the framework, logistics, and operations, elements of cyber-resilience and procedures on the policies, when considering threats and challenges in a changing environment. NATO is yet to decide on the resilience policy, as hybrid warfare is developing, at a time when smart defense of NATO nations are expected to achieve the goals and aims which are to be seen by the year 2020.

The cyber-attacks in Estonia of 2007 are still today the biggest and most organized electronic attack, with a duration period of several weeks, provided NATO with a motive and multipurpose task for years to come. NATO’s leadership was in fact correct in its judgment that (1) such an operational center and policy was needed, (2) its operational center would constantly be evaluating and evaluated, and would research on prospective evolutions in technology, malware, and cyber-security (3) that NATO requires resilience when considering the current or future threats and challenges.

The inauguration of its Cooperative Cyber-Defense Centre of Excellence (CCDCOE) in Tallinn Estonia in May 2008, led to a mission, which holds a clear vision and statement. It is yet to be “politically ratified” and adopted as a key core policy by Allies. Its raison d’être as stated is “to enhance the cooperative Cyber-Defence capability of NATO and NATO nations, thus improving the Alliance’s interoperability in the field of cooperative Cyber-Defence,” therefore reflecting on the key core elements to counter hybrid threats and be constantly resilience to strategic requests and needs. The vision is for the CCDCOE to become “a specialized and expertise center for NATO in cooperative cyber-defense” (CCDCOE, Training Catalogue, n.d.).

The domain of the cooperative cyber defense center in the framework of cooperative security within NATO focuses in the fields of research which include:

“Legal and policy elements”

Concepts and strategy

Tactical environment

Critical information infrastructure protection (NATO, 2016c)

The Centre’s core policy created an outcome of research and policy-orientation, as already analyzed. It was presented primarily as a first outcome, then accepted by the Supreme Commander Allied Command Transformation (SACT), deriving from a request of NATO HQ (Headquarters) and by the North Atlantic Council (NAC) level. This included Doctrine and Concept Development, Awareness and Training, Research and Development Analysis, and Lessons learned and finally Consultation.

In July 2018 during the Brussels NATO meeting, the Heads of States and Governments agreed to the opening of the cyberspace center as part of the new NATO command structure reform that provides more agility and assurances of operational preparedness, while ensuring force command operations and agility (Efthymiopoulos, 2013). The agreement includes a creation of policy and action reflecting key core issues including a framework policy for the cyberspace operations center of NATO to learn and coordinate in operations how to counter emerging challenges.

Results: NATO innovates with reflection to cyber-security

In terms of cyber-security, the Centre for Excellence in Tallinn continues to portray and project NATOs need for a methodological cyber-resilience policy. At NATO Brussels summit, cyber-security became operational. Therefore, NATOs cyber-defense policy and smart efficient methods while also requested for more interoperability agility and security resilience in the field of cyber-security becomes a core policy.

The attempt as an idea and method to reach out on cyber-security agility of forces for operations is not a new one. On February 6th and 7th 2009, NATO’s Science for Peace and Security (SPS) sponsored a workshop. It foresighted the possibility of cyber-security framework. Something we commend through this article: a framework strategy for operational and efficient cyber-security to become a core policy of resilience at NATO. The 2009 workshop titled “Operational Network Intelligence: Today and tomorrow” aimed at adaptation knowledge procedures considering the evolving and fast growing technology. It spoke about innovation and entrepreneurship. It talked about methodological approaches that may bring allies together, while bring cooperative sides together in investment through R&D opportunities.

Its overall purpose therefore was to introduce the possibility of innovation: “rethink present strategies and identify urgent measures to be taken in order to minimize the strategic and economic impacts of cyber-attacks” (NATO, 2009b). This was the level of anticipation at the time; considering future correlation of smart-defense with the policy of cyber-defense at its core. In 2019, innovation seems to be a sound but lone option; a process where through cooperative security and military and technological entrepreneurship NATO can move forward.

In 2019, considering the risk assessments on hybrid threats and challenges (Davis Jr., 2015), the need for better civil awareness and readiness, at a time of much needed cooperative defense, Allies have to decide for a robust long-term planning innovative and entrepreneurial strategy for current and future operations of NATO. Keeping in mind the need for strong success in field operations, including success in and at a multi-dimensional level of operations against all threats while making operations to be cost efficient with minimum human casualty numbers.

NATO increasingly recognizes that organized cyber-attacks seek to take advantage of “gaps” in the “system social and market matrix.” Therefore, it should be a request from member states to examine the increasing need for coordination of human factors related to the issues of electronic warfare, operational network, intelligence, and cyber-defense, whether for training, scientific exchange, and or operations (NATO Review, 2015).

NATO is currently using people involved in e-systems, security, IT engineers, researches, officers dealing with network operations and operational centres, as well as professional and academics, among others including military specialists. Specialists in the field on both a strategic and tactical levels should continue to be systematically involved at organized levels of research, sharing, discussion, and exhibition of outcomes, which will in turn enrich the abilities, capabilities, and capacities of rendering current smart-defense and cyber-security as a key and successful resilient and collaborative defense policy to NATO.

### UQ---Smart Defense---AT: No Smart Defense Now

#### Smart Defense is coming now---their evidence is outdated and doesn’t assume allied perception

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

As previously noted, cyber-security capabilities in a smart and resilient way is the “operational goal.” NATO members prepare well and also at joint levels. NATO’s Smart Defense,Footnote1 a policy framework for defensive tactical advice and operations, used to be the method that among others branded the need for a cyber-security policy. A cyber-resilience of NATO, which was adopted during the Warsaw Summit in July 2016 and reflective to the July NATO summit in 2018, expects allies to take continued actions through standardized procedures of protection effectiveness and also innovative openness and entrepreneurial attraction through NATOs respective institutions, centers of excellence, agencies, and its new cyberspace operations center that is to be inaugurated in Mons Belgium.

What is well known through policy analysis is that NATO military forces should reach to appropriate operational and tactical levels, so as to operate in and around “article and non-article 5 operations” (Sendmeyer, 2010)—meaning not only defensive-clause operations but also in counter-offensive operations (NATO, 2008b). Cyber-protection and cyber-security methods are needed, when defense of allies is associated with possible threats or challenges such as the one of ISIS.

#### Their evidence is snapshot, Smart Defense will soon be evident

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

In specific, a cyber-security strategy for NATO will enhance its innovation and creativity core of operations and methodologies against any kind of virtual threats. It will set standards, policy procedures, and recommendations. NATO’s strategy of cyber-security through its new Cyberspace Operations Centre, in Mons (Belgium) as decided in the Brussels Summit of July 2018 (Cyber-Space Operations Center Mons Belgium, 2018) unfolds options and opportunities, innovation, and entrepreneurship in operations efficiency and capabilities application. Current technological advancements and dynamisms through innovation and sustainable futuristic advancement will soon be evident.

### UQ---Tech Innovation

#### NATO’s proving its capable of innovative tech development now

Camille Grand 20, NATO’s Assistant Secretary General for Defence Investmen, Matthew Gillis, Defence Investment Staff Officer at NATO HQ, "Alliance capabilities at 70: achieving agility for an uncertain future", NDC Policy Brief No. 01, Jan 2020, <http://www.ndc.nato.int/news/news.php?icode=1408>

Blueprints for the future?

The future outlook for disruptive technology is not entirely negative. Two new initiatives show exceptional promise to invert traditional capability development models, while seizing upon the opportunities offered by new technology. They demonstrate vividly how NATO adapts.

The first is the Maritime Unmanned Systems Initiative. Here, 14 Allies have committed to a cooperative framework for developing and integrating unmanned systems into NATO’s defence architecture.2 The project is aimed at bringing autonomy and unmanned capability to bear in support of tedious and dangerous jobs at sea, including anti-submarine and counter-mine warfare. Beyond leveraging new technology, the project is also leveraging a “start up” mindset for agility and lean approaches. The project has benefi ted from experience drawn from industry, academia, and government, including Coca Cola and the Pentagon’s Defense Innovation Unit. This model has already paid dividends: less than a year after the fi rst commitment was taken, the largest-ever exercise of NATO unmanned underwater, surface and air vehicles took place off Portugal.3

The second initiative is the Alliance Future Surveillance and Control capability. In a novel example of obsolescence management, NATO leaders have committed to cooperate towards defi ning a replacement for NATO’s AWACS fl eet in anticipation of its retirement around 2035. The project launched in 2016 with a fundamental re-evaluation of NATO’s future needs, eschewing any assumptions that AWACS would simply undergo a “likefor-like” replacement. The project has since arrived at capability requirements that drive for an integration of surveillance and C2 across multiple domains. Allied industries have now been challenged to offer ideas on how NATO’s requirements could be fulfi lled by 2035. Up to six concepts are being sought in order to encourage a wide variety of innovative solutions, including those that leverage emerging and disruptive technologies.

Both of these projects are in their early steps. Nevertheless, their models are contesting the traditional approaches to defence acquisition by embracing disruptive technology, tapping into industry expertise, and leaving space for future capability growth. These projects offer promise for the future adaptability and agility of NATO capability development, and as such deserve close attention and support.

### Link Wall---2NC

#### Commitment---fully embracing emerging tech requires a defense posture that accounts for the uncertainty of future developments---broad acceptance of risk increases the demand for new tech innovations

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

In twenty-first century security affairs, NATO forces are required to be well prepared for possible rules of engagement at all levels and dimensions. They should be able to counter symmetrical and asymmetrical battles, threats or challenges, hybrid or non-hybrid. At the level of cyber-security and cyber-resilience and preparedness, scenarios, of possible attacks and battles, can be anticipated. Along the lines of the new cyber-space operations center, NATO should prepare operational methods for action, whether this is for defense or cooperation for cyber-space.

The use and necessity today of technology is limitless. So is the virtual world of defense and security, where technology and cyber-defense merge. These are the tools for action. Technology plays a key role in a global reach. Yet so does NATO, through the framework of a limitless technology applied in military operations. NATO uses technology to train, prepare, ready, deploy, and operate its forces. Technology for NATO works as tools with which the Alliance protects and defend, yet also is capable to counter-assault, with counter-measures where and when is needed, required, or decided.

Since the adoption of the NATO Cyber-Defense policy (NATO’s Cyber-Defense Policy, 2011), NATO trains its military and civilian assets for possible action against possible threats. NATO is constantly training its forces in cyber defense training can be achieved through national, bilateral even multilateral levels of NATO, through the association of member states, at the level of Centres of Excellence, such as the NATO Cyber-Defense Centre for Excellence (CCDCOE) (NATO, n.d.) and now through the Cyberspace Operations center in Mons Belgium. Training and exercises are now anticipated to expand and enlarge. So are multinational operations held through remote areas and locations. NATO is now to get more engaged in the field of cyber-defense, in both operations and tactics. It is anticipated within the Alliance that NATO is well prepared, both for current and future challenges, countering multiple and multileveled dimensions of cyber-attacks. Yet, it also holds an open option, if necessary, to conduct counter-offensives to prevent further escalation of cyber or military actions (Hughes, 2009).

NATO Missions, “will continue to require agile and interoperable, well-trained and well-led military forces” (Carayannis, Campbell & Efthymiopoulos, 2014). This new technological and operational environment through cyber-defense provides NATO with a new level of technological possibilities, new tools for use against possible threats but also protective “cyber-objectives.” Allies have an added policy, mission, and value. Ongoing and constant transformation through its operational and capacity building resilience, aims to reach in updated capabilities and political excellence, in 2016. NATO aims for well-coordinated missions in cooperation with and/or participation with other international organizations, when prompted to react on international threats or challenges. As such, NATO has the ability to continue to be a force and security provided in future potential of, what we may call it, the “online” security protection initiative against all possibly known threats.

NATO seeks excellence, in achieving the best smartest way to protect but also counter-attack. By “nature,” NATO exists to prevent and defend member states from attacks. Through smart ways and agile training, NATO can counter most known ways of interface (whether virus or virtual) attacks or even e-spying attempts.

#### Decision-making framework---centralizing decision gates through complicated management structures ensures capabilities will be over budget, late, and obsolete when delivered---government limitations get in the way of ‘business-led’ innovations

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

During the year 2018, there was a new security cultural security comprehension; it is considered as multi-leveled and multi-dimensional. In 2018’s NATO summit of July, allies evaluated current developments in cyber-security considering challenges, threats, but also opportunities. Evaluated current strategic and geopolitical challenges. They upheld methodological preparedness for network defense and operations and declared under the new NATO command structural reform the setting up of a cyberspace operations center, as part of the adapted command structure. Allies now request for more awareness and openness, innovation methods, and capacity building in cyber-security, considering changes in the market economy, more tangible and operational capacity building through R&D companies. Any decision, considering the changing nature of security and strategic market, should be “business-led” innovative-led, promoting sustainability and growth, market methods to uphold NATO’s relevance, while keeping the public informed. The public is keen on understanding the operational usefulness of the alliance, at a time of inside and outside NATO members’ landscape threats and challenges.

Defense capacity building for the twentieth century requires a modern way of thinking. It is about encouraging cooperative defense at the level of expected outcomes considering global but also regional risk assessments. NATO is still to enhance but also maintaining military capacities and military capabilities.

The new strategic concept of NATO requests the alliance to move forward. Twenty-first century needs and challenges require agility and compatibility of forces and force command at all levels, including network-centric operations and defense.

NATO forces, force command, technology, and methodological approach in military elements and standards cannot be or remain static. They need to technologically advance, progress methodologically innovate, to accommodate for the increasing need for multi-dimensional ways of security and defense. NATO needs to have interoperable, capable, and well-equipped technologically agile forces considering innovation and entrepreneurial thinking in a period of technological advance.

#### Line drawing---static methodologies prevent constant tech upgrades needed to stay prepared for future threats that are impossible to anticipate

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

In an emerging globalized world, where complexity may become a key characteristic in strategy and security, resilience will become an integrated part of NATOs policy orientation and application. New vulnerabilities and threats continue to emerge. Political pressure will require NATO leaders to take decisions about the organization’s future. Yet all agree that NATO is a necessity. As such, NATO should become more open, more adaptable, and more flexible. With more burden sharing, better smart budgeting, long-term planning, and operational application and continued success, NATO should continue be re-branded as an adaptive security organization that does more to offer security and strategic alignment to truly current but also future challenges and threats, that we may not yet anticipate or think of.

In the not so long past, such similar actions reaffirmed by the Heads of States, included among others, the Treaty of London in 1990 Summit, to the 1994 Summit in Brussels, and in 1999 over its 50th year anniversary Summit in Washington, to the immediate decisions taken in 2001 after the terrorist acts in the USA (NATO, 2001b) to its 60th anniversary, which was held in Strasbourg and Kiehl accordingly in April 2009 to the Chicago Summit of 2012 and the Wales Summit of 2014, which added value to the Alliance and Allies reaffirming NATOs long-term necessity but now also strategic resilience to multi-dimensional challenges and threats.

Vulnerabilities and threats considering multidimensional challenges such as cyber-security require NATO to be truly, strategically and operationally agile. It requires NATO to be adaptable to conditions unforeseen.

Considering technological advancements, we are yet to acquaint ourselves, our institutions, governments, and international organizations with true phenomena of a new, yet networked global society. In this borderless society, where electric grids, information, or installations failures may have in the past solely affect a country, now affect a region and possibly a larger area. Our abilities are limitless to point out challenges and face them. We also have the ability to innovate through methodological approaches and security cooperation utilizing the constant upgrade of technology. However, when decisions come to being, this may not be easy.

### Link Wall---General

#### Collective defense is the foundation of Smart Defense---limiting our commitment hurts resiliency, duplicates efforts, and prevents interoperability

Marios Efthymiopoulos 19, PhD from the University of Crete in Security and Strategic Affairs on NATO issues and NATO-Russia relations, Chairman of the Board of Advisors of Strategy International, 6/24/19, "A cyber-security framework for development, defense and innovation at NATO", Journal of Innovation and Entrepreneurship, Volume 8, Article 12, https://innovation-entrepreneurship.springeropen.com/articles/10.1186/s13731-019-0105-z

NATO’s concept of cyber-defense in 2019

It was NATO’s Military Committee decision to adopt a “Cyber-Defense Concept” (Efthymiopoulos, 2008e). The Committee’s aim was and still is to deliver business continuity and military resilience. As NATO is a provider of collective defense and as a collective organization in a globalized and currently unsafe e-world, it needs to be agile. In an environment of insecurity, the Alliance’ delivers new policy results. Taking into perspective new forms of asymmetrical threats, such as cyber-attacks.

Historically, the 2002 Prague Summit first marked NATO’s tasking authority committee with regards to all activities that should be held in relations to cyber-defense. As technical achievements were delivered, so policy-makers delivered policy results on cyber-defense. That is why, Allied leaders during the Riga Summit of 2006 acknowledged the need to include these as is stated on its decisions at the Press Communiqué: (1) to protect NATO’s operational information systems, and (2) to protect its allied countries from any e-, or in other words cyber-attacks by new forms and means developed by NATO’s Allied Command Transformation (ACT) In Norfolk Virginia.

The output of the informal Meeting of the Ministers of Defense in October 2007 of NATO (NATO Defence Ministers Meeting, 2007) gave way to the inauguration of NATO’s Center for Excellence (COE), which at a later stage got accredited to have become the Allied Command Transformation on cyber-defense, named as Cooperative Cyber-Defense Centre of Excellence, CCDCOE (NATO, 2008a). It was based on the concept and early understanding of cyber-resilience for NATO’s future policies in countering challenges and threats, as was agreed by NATO’s Military Committee.

The central and final decision-making role over the policy of cyber-defense however is the North Atlantic Council (NAC), which accordingly is led by Heads of State and Governments. This is the highest deciding political authority which decides, creates, and overviews policy. It also evaluates, considers, and adopts NATO’s policies and activities with regards to political and military affairs or standing issues on challenges and threats, among others. Below the NAC, is NATO’s Consultation Control and Command Agency (NC3A) (NATO NC3A, 2002) now transformed to the NCIA agency (NATO, 2008a) and the NATO Military Authorities (NMA). The latter authority has implementation as its major task (NATO’s Cyber-Defence policy, 2008).

The implementation of NATO’s cyber-defense policy is considered as the second most important decision by now, once the decisions are taken by the NAC. The “Concept of Cyber-Defence” “adds practical action programmes, to fit within the overarching policy” (NATO, 2009a). The “Cyber-Defence Management Authority” that is tasked upon its policy concept “brings together the key actors in NATO’s Cyber-Defence activities.” Its aim is to manage and support all NATO communication and information networked systems and individually allies upon request (NATO, 2008c).

NATO’s policy creation and activity is “encouraged” by Allies. The aim is to adapt the alliance to the new strategic and security environment that is “hybrid” and thus the creation of the cyberspace operations center in Mons in Belgium. To engage as many as possible governments, industry-related market companies, and individuals. In accordance to its best practice policy, NATO considers that its “operational forum” can and should be considered as the best joint operational cooperation between states and market, as to also avoid duplication of efforts and use the necessary global knowledge to achieve interoperability of force action and command also in cyber-space.

Practically, in military policy, implementation, or operational areas, NATO has adopted “three phases of practical activity and cooperation”: the initial phase includes a NATO Computer Incident Response Capability (NCIRC). It was established as “interim operating capability” for NATO to build up on both security risk and manage the element of cyber-threats. Its second phase involved an ever more realistic and pragmatic perspective that required the coordination of all initial “offering” states to the attempt to establish a cyber-center (under the NATO agreement between states of a voluntary national contribution—VNC), in bringing the NCIRC to a full operational capability (NATO, 2008c).

New and innovative policies were adopted. They were proposed and came to effect (well-known procedure of internal NATO working process) until the adoption of “MoU”; a memorandum of understanding was drafted and proposed to NATO, by a sponsoring state which would establish a center for cyber-training, in this case in Estonia.

From that point on, it became an administrative decision of the Allies, that once the aforementioned stages would be put into effect, then a third phase would come into existence. Needless to say, this third phase was a complete implementation and rule-based operational procedure that would soon enough bring about into existence NATO’s request for technological agility and resilience, which is finalized at the Warsaw Summit of July 2016. It consists of incorporating—lessons learned—from the prior two phases as using new and latest cyber-defense measures (use of new technology and getting more knowledge on the security environment), in order to enhance cyber-defense posture. Once the third phase was evaluated, the Allied Command Transformation (ACT) decided, to accredit the operational center—in this case the Cooperative Cyber Defense (CCD) COE (Estonia), what is called as a “Centre of Excellence”. In turn, this resulted to the inauguration of the CCDCOE by May 2008.

#### Limiting Article 5 commitment to hybrid threats undermines cyberdefense integration

CDR Wiesław Goździewicz 16, Legal Advisor NATO Joint Force Training Centre, “From Riga to Wales. NATO’s Road to Collective Cyberdefence”, NATO Road to Cybersecurity, The Kosciuszko Institute, https://ik.org.pl/wp-content/uploads/nato\_road\_to\_cybersecurity\_the\_kosciuszko\_institute\_2016.pdf

The Wales Summit Declaration8 was a major step forward in acknowledging the challenges posed by complex cyberattacks. It was the first official document in which the Member Nations of the Alliance confirmed the possibility of a cyberattack to cross the threshold of an armed attack and thus become the basis for invoking Article 5 of the North Atlantic Treaty. It was reiterated that cyberthreats and attacks would continue to become more common, sophisticated, and potentially damaging. In Paragraph 72, the Alliance Nations declared that:

“Cyberattacks can reach a threshold that threatens national and EuroAtlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO’s core task of collective defence. A decision as to when a cyberattack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.”

This clearly demonstrates the Alliance’s view whereby cyberattacks can cross the threshold of an armed attack, allowing individual or collective self-defence to be invocated under both Article 51 of the UN Charterand Article 5 of the North Atlantic Treaty. Moreover, for the first time since NATO took on the topic of cyberdefence in 2006, it was explicitly stated that cyberdefence became part of the Alliance’s collective defence tasks and efforts.

The Member Nations adopted the Enhanced Cyber Defence Policy (ECDP) which reaffirms the principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence and clearly states that “(…)the fundamental cyber defence responsibility of NATO is to defend its own networks, and that assistance to Allies should be addressed in accordance with the spirit of solidarity, emphasizing the responsibility of Allies to develop the relevant capabilities for the protection of national networks.” The ECDP recognises the applicability of international law to cyber operations, including the International Humanitarian Law (IHL) or the Law of Armed Conflict (LOAC).

The Nations committed themselves to further develop their national cyberdefence capabilities and enhance the cybersecurity of their networks, upon which the Alliance depends. NATO’s top priority for cyberdefence is the protection of NATO-owned communications and information systems (CIS); however, the Alliance will assist the Nations in defending their national networks considered critical for NATO’s missions. For this purpose, the Alliance cooperates with national authorities to ensure an appropriate level of cyberdefence of national CIS. Such cooperation is being formalised in Memoranda of Understanding (MOUs) signed between the Cyber Defence Management Board and the respective nations. Cyberdefence MOUs are based upon a template developed in the Cyber Defence Action Plan in line with the principles of the ECDP. They set the foundations for mutual support in the area of cyberdefence, including information sharing, participation in training and exercises as well as the provision of reciprocal assistance in the form of intelligence and “manpower” (CIS specialists and cyberdefence experts). The Czech Republic was the first NATO Nation to sign such a MOU on 12 October 2015.9 Assistance to Allies may be provided by one of the Rapid Reaction Teams formed by the NCIA as part of the Alliance’s collective cyberdefence capability.10

The Wales Summit Declaration further provided for a continued integration of cyberdefence into NATO operations and operational and contingency planning, as well as the enhancement of information sharing and situational awareness among Allies. The key role of partnerships in addressing cyberthreats was stressed.

Also the ECDP requires NATO to include cyberdefence aspects in the defence planning process. This has been achieved by implementing respective cyberdefence annexes in Operations Plans (OPLANs) developed for real-life operations, training and exercises as well as contingency plans. The training and exercise programme has grown to include cyber-specific exercises such as Cyber Coalition and Locked Shields. In addition, an extensive cyberdefence play has been incorporated into more “classic” training and exercises, including the biggest NATO exercise over the last decade – Trident Juncture 15 and Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise (CWIX), to which the Joint Force Training Centre has been the proud host for the last five years.11

One of the most important aspects of the NATO ECDP is cooperation in broad terms: with NATO Nations (as described above), Partner Nations, international actors such as the UN and the EU, industry and academia. Cooperation with industry has been formalised in the NATO Industry Cyber Partnership (NICP), which was founded and endorsed by the Alliance based upon the conclusion that NATO and industry faced shared risks in cyberspace, and that addressing these challenges required new frameworks for action. Within the NICP framework, the NCIA has launched the cybersecurity incubator concept tasked to develop a new model for NATO-industry cooperation with the aim to decrease the time required for NATO to develop its cyber response capabilities, based upon the results of research and development programmes already run by industry and academia.

There are many other cooperation frameworks such as the Cyber Information and Incident Coordination System (CIIS), a web-based application developed for sharing cyberdefence information within a trusted community and available to all NATO Nations and Partner Nations as well as commercial organizations.

NATO does not develop offensive cyber capabilities. Although the Alliance focuses on defence against cyberattacks, it does not preclude particular Member Nations from developing their own national offensive cyber capabilities. In fact, there are nations who openly admit they pursue such capabilities involving “(…)countering (disorganising, jamming and destroying) the sources of threats (active defence and offensive actions) (…)”.12 As a matter of fact, NATO Rules of Engagement13 in Series 36 (Information Operations) envisage the possibility of conducting offensive computer network operations (namely Computer Network Attacks – CNAs); however, none of these offensive ROEs have been authorised so far by the North Atlantic Council in operations or exercises.

This short text hopefully illustrates how NATO’s approach to cyberdefence has evolved over the last decade to culminate in a clear and unambiguous declaration that cyberattacks can trigger the invocation of Article 5. While the Alliance is committed to assist Allies in their defence efforts, it encourages the Member Nations to develop their own cyberdefence capabilities in the spirit of Article 3 of the North Atlantic Treaty. This evolutionary approach should be continued to ensure the adaptation of the Alliance’s cyberdefence policy to new trends in cyber operations, including the development of response options to e.g.:

1) cyber actions amounting to armed attacks;

2) the possibility of a broader application of cyber means and methods of warfare in future conflicts;

3) terrorist acts with the use of cyber means.

Adaptability and flexibility as well as a broad range of response options are a must in the world where the vulnerabilities of critical infrastructure are no secret and neither is the reliance of countries on critical infrastructure which in many cases is shared between two or more countries.

### Link Wall---Baltics

#### Baltic participation in tech innovation to counter hybrid threats drives multilateral adoption throughout Europe

Justinas Mickus 19, Associate Analyst of Vilnius Institute for Political Analysis, and Piret Kuusik, International Centre of Defence and Security Junior Researcher, October 2019, “The Baltic Risk Landscape,” https://efpi.icds.ee/wp-content/uploads/sites/18/2019/11/Mickus-Kuusik\_The-Baltic-Risk-Landscape\_October-2019.pdf

To an extent, then, the developed expertise in combatting cyber threats can and already has enabled the Baltic states to set multilateral standards and craft collective policy solutions in the field. And yet, with the increasingly widespread appreciation of hybrid and next-generation threats, the comparative advantage the Baltics have today will likely decrease in the future. Should Baltic politicians wish to further pursue leadership in cyber and hybrid security, they will require further policy innovation (a similar note could be made about the self-declared Baltic expertise on Russian/Eastern Neighborhood questions more broadly).

The Baltics, certainly, may also focus on other areas in which they play a unique role and boast unique expertise. Today, individual Baltic states have made significant inroads in developing notable expertise in e-governance (Estonia) or fintech (Lithuania). Survey respondents from Latvia and Estonia also demonstrate high appreciation for and diverse understanding of the impact the rising pace of technological change is likely have on Baltic politics. For both sets of respondents, this trend ranks among the top three and is connected with various economic, societal, and security risks (by contrast, increasing cyber-dependence is primarily through the security lens).

Whether they choose to further develop their hybrid and cyber capabilities or expand their focus to different fields, the Baltic states stand to benefit from international cooperation. As continuous policy innovation requires new inputs, seeking diverse international partnerships can greatly augment the policy instruments currently employed by the Baltic states. For example, should the Baltic governments focus on the trend of ageing population (among the experts surveyed, it ranked as the most important trend in the Baltic region), the could consult the expertise and experience of Japan, which has recently developed an ambitious strategy of tackling the transformation into a digital society for an ageing population.11

ACTIVE AND CONSTRUCTIVE MEMBERSHIP

Unique expertise alone is not sufficient for small states to shape the international order with the use of postwar institutions – there is a difference between being a one-issue state and the leader on the issue. Small states must simultaneously be active and constructive partners to other members of the core group of the postwar order. As their institutional innovations need the assent and backing of greater powers to have any tangible effect, fostering stable and productive partnerships with key allied powers to secure their buy-in is a necessary tactic for small states.

#### NATO’s hybrid warfare planning is concentrated in the Baltics.

Eoin Micheál McNamara 2016, PhD researcher at the University of Tartu where he has lectured in transatlantic relations, associate fellow at the Latvian Institute of International Affairs in Riga, “Securing the Nordic-Baltic region,” 17 March 2016, https://www.nato.int/docu/review/articles/2016/03/17/securing-the-nordic-baltic-region/index.html

Russia’s illegal annexation of Crimea in March 2014 and its military actions in Ukraine have led transatlantic policy-makers to reassess collective defence arrangements across what is frequently referred to as NATO’s “eastern flank”. Extending north partially beyond the “eastern flank” is a region that comprises eight Nordic and Baltic states, which have become increasingly interdependent in security terms. The region is of rising importance in the context of Europe’s changing security order – and defence and deterrence is set to be high on the agenda at NATO’s summit meeting in Warsaw, Poland, in July.

NATO has a strong role in coordinating closer security ties between the region’s states. Finland and Sweden are not members of the Alliance and are therefore not covered by NATO’s collective defence clause. However, the Allies are working closely with both countries – two of NATO’s most active partners – to assess security in the Baltic Sea region, to expand exchanges of information, including on hybrid warfare, coordinating training and exercises, and to develop better joint situational awareness.

The prospects are positive for improved NATO-Nordic-Baltic defence cooperation, yet a number of important challenges need to be overcome. The region will test NATO’s flexibility in strengthening defence ties among its members and crucial partner states.

#### Bolstering hybrid response in the Baltics is the first step towards broader NATO/EU adoption

Andrew Radin 17, political scientist at the RAND Corporation, 2017, “Hybrid Warfare in the Baltics: Threats and Potential Responses,” https://www.rand.org/content/dam/rand/pubs/research\_reports/RR1500/RR1577/RAND\_RR1577.pdf

Improving the response to potential Russian covert action can be thought of in three phases: detecting and attributing Russian action, strengthening the capacity of the Baltics to respond, and formulating an effective and appropriate EU and NATO response.

Better intelligence gathering and coordination and a clearer understanding of the signs of Russian covert aggression can help bolster defenses against active subversion. U.S. Air Force assets, such as unmanned aerial vehicles and ground-based radars, could be beneficial at filling gaps in these countries’ existing intelligence, surveillance, and reconnaissance capabilities, both for covert action and conventional warfare.7 NATO is also currently undertaking several initiatives to improve intelligence and coordination related to Russian covert action, including developing shared indicators and warnings, NATO Force Integration Units (NFIUs), and combined exercises. Although NATO has made progress in developing institutions for intelligence sharing, NATO’s structures and processes for intelligence sharing remain cumbersome and dependent on often-reluctant nations to share.8 Given NATO’s slow progress in this area, further developing bilateral intelligence sharing between the Baltic countries and the United States or other NATO countries could be valuable. Additional research could also contribute by identifying the signs and mechanisms of past instances of large-scale Russian covert activities in Georgia, Crimea, and eastern Ukraine. So far, there is little open source information about how to differentiate between “everyday” Russian exercises and influence operations and the start of a large-scale campaign mirroring the operation in Crimea. More clearly identifying the modus operandi of Russian agents would help to separate out the cases that justify a NATO deployment and those that might not.

The capacity of the Baltic countries to counter covert action can certainly be improved. U.S. special operations forces have conducted extensive engagement with their Baltic counterparts, to the point that there is a sense of saturation, especially given the small size of the Baltic special operations forces. Additional research may be beneficial to help identify gaps in the Baltic countries’ capacity, including within civilian agencies, and to conduct targeted missions that could offer more focused benefits. Support for the Baltic states to counter covert action may also strengthen their ability to resist Russia in the event of an invasion.9 The U.S. Air Force may be able to directly assist with the development of technical capabilities for border control, air and maritime domain awareness, and intelligence gathering, including assistance with acquiring unmanned aerial vehicles, radars, and other sensors. Another specific area where the United States may be able to offer assistance is in planning exercises and war games to improve contingency planning and coordination, especially in Latvia.

Finally, the United States, NATO, and the Baltic countries can do more to think practically through how a response to Russian covert action would proceed. The 2014 Wales Summit focused on the development of greater “responsiveness” through the Readiness Action Plan and the creation of the Very High Readiness Joint Task Force (VJTF). However, it remains uncertain how these new, more responsive forces would be employed if there was warning of a significant Russian covert (or conventional) military action in the Baltics.10 While the development of the VJTF and implementation of the Readiness Action Plan is complex and will take time, it is highly beneficial for the United States and other NATO allies to think through on a practical level how a high-readiness forces would deploy and be employed in the Baltics, and how they would coordinate its actions with the Baltic security forces.

### Innovation IL---K2 Tech Edge

#### NATO innovation is key to maintaining the tech edge against competitors while preserving shared Allied values

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

Sceptics will say this would present big tech with too many opportunities for mergers and acquisitions and thus create monopolistic risk. They might be right and clearly incentives for all parties would need to be found. But, if we are to win the technological adoption race built upon liberal democratic values, we need to use every advantage we have.

To utilise, adopt and scale these technologies effectively, we must have at the forefront of our minds the need to work at the speed of relevance rather than the speed of approval. This means new ways of financing technologies, interacting with tech firms both big and small, and much more agile acquisition models, which carry the empowerment and incentives to those responsible for equipping the Alliance. Such a cultural shift will not be easy – but innovation rarely is.

As we look towards NATO 2030 and heed Eisenhower’s words of achieving both security and solvency, while noting that the foundation of military strength is economic strength, a resilient innovation pipeline that leverages our comparative advantage, creativity and capital will be critical to the Alliance maintaining its technological edge built on shared Allied values.

### Innovation IL---NATO-Led Key

#### NATO is key to innovation---fragmenting efforts won’t means we lose the tech edge to competitors

#### NATO focus has a stronger effect on innovation priorities

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

But before we get to commercialisation, we need to create the direction of what it is we wish to see commercialised. Technological disruptive innovation does not just happen. It starts with a mission-oriented vision, where measuring risk is impossible and only uncertainty reigns. It requires bold moves that will signpost the future; the confidence to place big bets on technology not yet invented; and an ability to pick winners – all of which must be underpinned by persistent engagement, encouragement and enlightenment. Since the end of the Second World War, only one entity has taken-on such uncertainty: Allied governments (see image below).

Step 1: agree innovation priorities among Allies

The first step towards fixing the fragmentation of Allied disruptive innovation is for Allies, through the NATO framework, to focus on agreed innovation priorities. This will allow them to pick winners and invest public patient capital – the private sector is unlikely to invest venture capital as the risk is simply too high (nations tend not to go out of business and can take on such uncertainty). This direction and investment will help to maintain NATO’s overarching technological edge. Indeed, as Keynes and Weber argued, the ability to make things happen that otherwise would not needs a combination of technological, policy and bureaucratic skills matched by investment

#### Networking is key to maximize innovation

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

Step 2: leverage the comparative advantage of the Alliance

If Allies are to achieve most defence at less cost with least delay built with wisdom and efficiency, then it is logical to leverage those natural advantages that geography and skill sets afford NATO member states. A network of the finest universities across the Alliance should be established and resourced to allow cutting-edge multinational research to take place across multiple disruptive technologies simultaneously. Perhaps Stanford could lead on relevant AI research, while Delft and the University of Chicago partner on quantum; maybe Imperial College London looks at biotechnologies with Johns Hopkins University, while Tallinn University centres its efforts on next generation cyber defences; and the École Polytechnique and Massachusetts Institute of Technology examine future telecommunication needs.

The point is Allies will need to leverage such networks of universities in conjunction with national government research labs to provide maximum innovation coherence. The diversity of multinational, multi-disciplined defence and security innovation research teams, which NATO can engender, is a huge asset and is the Alliance’s competitive advantage.

#### Solves foreign ownership concerns

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

Utilise, adopt and scale

Where the first stage of NATO’s innovation pipeline should centre on the creation of disruptive innovative technologies, stage two is all about their utilisation and adoption at scale.

Utilisation

This is where initial public venture capital (VC) entities, such as in-q-tel, NSSIF, DefInvest and SmartCap, can help ‘crowd in’ trusted private venture capital to provide safe financing to NATO’s fledgling start-ups, thereby minimising their susceptibility to nefarious foreign direct investment. This issue is impacting many start-ups as they raise funds and carries implications when they wish to export their products but may not be able to, due to unfriendly foreign ownership and technology transfer concerns raised by Allied governments.

In addition to Venture Capital entities supporting the trusted financing of Allied start-ups, innovation accelerators – in combination with elite universities, and supported by Allied defence professionals (operators, investors and procurement experts) – can help provide the necessary ‘polish’ to start-ups and their value propositions. This will create the necessary ecosystem to maximise the likelihood of commercial success. The United States’ Air Force Ventures is an interesting model of this approach, which helps to acquire new start-up products at speed without being bogged down by acquisition bureaucracy.

#### Startups need NATO to get off the ground

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

Adoption

But even when dual-use disruptive innovation is commercialised, turned into prototypes and the product/market fit is achieved, the challenge of getting initial contracts from customers (both government and commercial) remains. Cash is king for young companies, as they do not have the financial reserves to work through long acquisition processes often associated with Allied governments. If start-ups cannot close deals in a matter of weeks and months rather than quarters and years, then they would not attempt to (opportunity cost).

Now, some commentators may argue: Why spend so much time discussing start-ups? Traditional large armaments companies can be innovative. Why go through all this effort for tiny companies that may or may not make it?

The reason is simple: the competition and creativity generated by start-ups is good for the Allied defence ecosystem. Allied open democracies and open educational models bring about levels of creativity which other forms of government are unable to do. This maximises disruptive innovation efforts and, as such, forces incumbents (large companies) to compete with new, fresh thinking – it builds resilience.

Such creativity and disruption is NATO’s competitive advantage. Therefore, NATO needs to adapt its acquisition models to accommodate start-ups, their timelines and their potential. This fundamentally means our acquisition professionals should be empowered to take measurable risk. As one Ally’s legislative body recently remarked: “Defence stakeholders must integrate the risk culture, which is the only way to both enable innovation in defence and to very quickly capture dual or civilian innovation. Acculturation to innovation is a priority.”

Scaling

If we have managed to commercialise new technology, adopt it quickly as a prototype and now wish to scale, how might this be done? Big tech could have a role to play here. In May, it was reported that, in the first quarter of 2020, Facebook, Apple, Amazon, Alphabet and Microsoft spent over 29 billion US dollars on research and development (R&D). That is more than the entire 2020 NASA budget and represents a 17 per cent increase on the same time period last year.

In November 2018, the US Congressional Research Service noted: “In 1960, the United States accounted for 69% of global R&D, with U.S. defense-related R&D alone accounting for more than one-third of global R&D (36%). Additionally, the federal government funded approximately twice as much R&D as U.S. business. However, from 1960 to 2016, the U.S. share of global R&D fell to 28%, and the federal government’s share of total U.S. R&D fell from 65% to 24%, while business’s share more than doubled from 33% to 67%. As a result of these global, national, and federal trends, federal defense R&D’s share of total global R&D fell to 3.7% in 2016.”

Big tech has the resources and wherewithal to be able to scale new technologies at speed. They could partner with successful start-ups, perhaps through a joint venture or an Alliance-wide public-private partnership, to provide those scale-up skills that start-ups lack (for example, compliance, legal support, production on mass, intellectual property protection) without necessarily acquiring these young companies.

### Innovation IL---AT: Gov Innovation Fails

#### Gov innovation works

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

As the image above shows, governments have done this before and the technologies created (internet, GPS, touchscreen et al, which fed into the building of the iPod and iPhone) have had a huge impact on the way we live. However, for all those successes, there will have been many failures and this is where Allies will need to get comfortable. To quote one anonymous Allied defence innovator: “if our success rate begins to go above 35 per cent, I start to worry. It means we’ve stopped taking big enough risks.” Indeed, obvious research areas Allies might collaborate on include the follow-on to 5G or the technology needed to enable total supply chain assurance, for example.

#### Yes capabilities

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

In aggregate, the Alliance has an abundance of world-class academic institutions, the finest scientific researchers, amazingly creative start-ups and a mature well-resourced financial eco-system. These constitute the core ingredients, which, when combined and focused, can solve dual-use, ‘tough-tech’ problems – that is, challenges facing both defence and non-defence sectors, such as augmented reality and quantum computing.

#### Yes incentive

Rob Murray 20, head of the Innovation Unit in NATO’s Emerging Security Challenges Division, MSc, ISR Management, University of Lincoln, MBA, The University of Chicago Booth School of Business, MA, International Policy and Diplomacy, Staffordshire University, 9/1/20, "Building a resilient innovation pipeline for the Alliance", NATO Review, https://www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/

A dual-use model is important for disruptive defence innovation because when we eventually get to commercialising such tough-tech breakthroughs, Allies will need start-ups and tech firms to maximise the reach of their products by looking at ‘total addressable problems’ rather than ‘total addressable markets’. In other words, we should not want start-ups building the next wave of technology to have governments as their only customer. We want such technologies to benefit society too and therefore have civil, commercial use. Such commercial use then drives the subsequent development of said technology, pulling the government-side along with it, which means better products and technology all round – building defence with wisdom and efficiency.

Indeed, dual-use potential will help align the incentives of our researchers, entrepreneurs and finance communities as the prospective commercial upside (problem) will be big enough for them to undertake the investment of commercialisation. The geopolitical advantage such disruptive innovation fosters (picking winners via big bets on the next breakthrough) will also be large enough to allow for its creation via early stage patient public sector capital investment.

### Innovation IL---Commitment Key

#### Commitment generates urgency---motivation gaps risk military failure

Paul Bernstein 19, a distinguished research fellow at the Center for the Study of Weapons of Mass Destruction (WMD Center) of the National Defense University in Washington, DC, ““Innovating” Versus “Out-Innovating”: Innovation as a Form of Strategic Competition”, Getting Innovation Right, Center for Global Security Research, Lawrence Livermore National Laboratory, Sept 2019, https://www.osti.gov/servlets/purl/1635772

Second, we need a sense of urgency and the means to accurately assess what others are doing. Russia and China are committed to developing leading-edge military technologies and fielding “high-tech forces” in part because they see U.S. dominance as an existential threat. They are highly motivated. It is not clear the United States is as sharply motivated, which creates the potential for a focus or commitment gap. Closing any such gap is something leadership should pay attention to; otherwise it may take a crisis or a military failure to generate the necessary sense of urgency.

### Innovation IL---Integration Key

#### Integration is key---we need to incorporate all elements of innovation to outcompete great powers

Paul Bernstein 19, a distinguished research fellow at the Center for the Study of Weapons of Mass Destruction (WMD Center) of the National Defense University in Washington, DC, ““Innovating” Versus “Out-Innovating”: Innovation as a Form of Strategic Competition”, Getting Innovation Right, Center for Global Security Research, Lawrence Livermore National Laboratory, Sept 2019, https://www.osti.gov/servlets/purl/1635772

Third, we need an integrated approach. A dynamic approach to innovating for operational advantage requires taking account of all forms of innovation, determining the appropriate mix for the types of conflicts the armed forces are likely to engage in and the specific operational challenges they will need to overcome. Innovation encompasses not only technology but also operational concepts and organization/ process. Military innovation and transformation leaders have long argued against an overemphasis on technology at the expense of other factors. Typically it is some combination of technology, concepts, and organization that provides a basis for breakthroughs. Often we are reminded of this when an adversary demonstrates it.

High-end regional war is generally the default lens through which we view requirements for innovation and it may be true that the bulk of defense innovation will be directed at this problem. But the spectrum of conflict also includes hybrid warfare (a mix of regular and irregular armed conflict) and coercive activities short of armed conflict (“political warfare”)—modes of conflict that are not entirely new, but whose contemporary manifestations are indeed novel and for which the United States generally seems poorly prepared. We cannot dismiss the requirements for innovation in these aspects of great power competition, not least because they may lead us down pathways much different from those shaped by the demands of highend regional war.

The following matrix may be useful as a very simple way to visualize the “battlespace” for innovation.

It is worth noting here that political warfare may be somewhat anomalous when considered as an arena of great power competition. In this domain, the goal of the United States and its partners is not to out-innovate adversaries so as to build the more advanced toolkit for political subversion, social division, economic warfare, and coercion. Rather, the West’s goal is to greatly improve the ability of liberal states to reduce their vulnerability to such strategies and actively resist them. This is a somewhat different context for innovation, but an important one given the strategic stakes.

### Innovation Impact---China AI

#### China AI competition escalates

Calum Chace 20, co-founder of the Economic Singularity Foundation, global keynote speaker about AI, MBA, Cranfield University, 6/30/20, "Thucydides And The Dragon: Artificial Intelligence And Sino-US Rivalry", Forbes, https://www.forbes.com/sites/calumchace/2020/06/30/thucydides-and-the-dragon-artificial-intelligence-and-sino-us-rivalry/#1c7a93d94fc1

From Cold War to Code War?

The most dangerous source of conflict could be China’s determination to catch up with and then surpass America as the leading developer of AI, our most powerful technology. Some fear that the Cold War between the two nuclear superpowers could be followed by a Code War between its two AI superpowers.

Taiwanese venture capitalist Kai-Fu Lee, a former Google and Apple executive, argues that China will overhaul the US in AI because it has more hard-working and aggressive entrepreneurs and researchers, and also because it has a disregard for privacy which allows its researchers to amass more data. “If data is the new oil, China is the new Saudi Arabia”, as one critic put it.

It is true that the 9-9-6 work ethic (72 hours a week) makes Chinese startup scene a highly competitive one. Many Chinese students no longer want to stay in the US when they finish their degrees in computer science. They are keen to return home and get rich there.

Do Chinese people care about privacy?

It is also true that China’s attitude to privacy distinguishes it from the US, and even more from Europe. The Social Credit system being pioneered today has the potential to become a level of government surveillance that would make Big Brother jealous. This is happening partly because the communist party wills it so, and resistance is pretty much impossible for most citizens. It is also partly because corruption is endemic and severe in China, and levels of trust outside family networks are low. A system which punishes anti-social behaviour swiftly and effectively is less resisted in China than it would be elsewhere.

But we should not over-state the extent to which being oblivious to privacy issues is a killer app. China watcher JJ Ding argues that Chinese people do care about privacy, and that the government knows it cannot take their acceptance for granted. The US tech giants still have a significant lead in technology and expertise, and they still have momentum. AI is increasingly a duopoly between China and the US, not an emerging Chinese hegemony.

The US managed to avoid the utter disaster of full-scale military confrontation with the Soviet Union, and in many ways its relations with China are much closer, which should make confrontation less dangerous. The US economy is less open than those of most developed countries – trade accounts for 27% of US GDP, compared to 61% for the UK, and 33% for China. But the US and Chinese economies are far more entwined than America’s ever was with the Soviet Union. GM sells more cars in China than in the USA and Canada combined, and Apple, Qualcomm and most other large US companies are similarly exposed.

Avoiding the splinternet: a role for Europe

Trump’s populist attacks on Huawei won’t kill it, although they could certainly curb its growth, and perhaps shrink it for a while. In the longer run they could easily have the perverse effect of damaging the US tech sector: China may decide that America is an inherently untrustworthy partner, and make the very heavy investments of time and treasure required to wean itself off US suppliers, and build its own chip industry, for instance. They could lead to “the splinternet”, a fracturing of the world’s technology ecosystem into two distinct communities, which would make global co-operation harder, and provoke mutual fear and suspicion.

War between China and the US (or NATO) is the worst possible outcome, but at this stage it still looks unlikely. Both the US and Chinese governments must walk a tightrope between pursuing their legitimate grievances on the one hand, and provoking outright hostility and communications breakdown on the other. This requires wisdom and diplomatic skills which are not prominently on display in both Beijing and Washington at the moment.

It would help if there were three AI superpowers, not just two. AI is not a race, as there is no finish line, and unless the internet splinters completely, the advances made by any party help everyone. But at the moment, Europe is barely involved. That ought to change, and soon.

### Innovation Impact---China Quantum

#### China quantum competition escalates

Arthur Herman 19, director of the Hudson Institute's Quantum Alliance Initiative, 11/10/19, "The Quantum Computing Threat to American Security", Wall Street Journal, https://www.wsj.com/articles/the-quantum-computing-threat-to-american-security-11573411715

Google announced last month that it had achieved "quantum supremacy," demonstrating the potential of a new kind of computer that can perform certain tasks many orders of magnitude faster than the most advanced supercomputers. It's a crucial moment for America's national security, which depends on winning the race to do what quantum computers will do best: decrypt the vast majority of existing public-key encryption systems.

Google reports that its quantum computer, dubbed Sycamore, solved a mathematical calculation in 200 seconds that would take a supercomputer 10,000 years. IBM, a quantum competitor, asserted that Google's claim of supremacy is overblown, and that the world's most powerful classical computer, the Summit OLCF-4 at Oak Ridge National Laboratory, could have done the same calculation in 2.5 days—roughly a thousandfold difference rather than 1.5 trillionfold. Still, quantum computers are no longer science fiction.

To process information, digital computers use bits, essentially switches that can be either off or on, corresponding with the binary digits, 0 and 1. Quantum computers employ "qubits," which use the probabilistic nature of quantum physics to represent any combination of 0 and 1 simultaneously, enabling them to encode more complicated data.

Their computing power grows exponentially as the number of qubits expands. Sycamore's 54-qubit chip allowed it to outcompute the best supercomputer. A 2,000- to 4,000-qubit quantum computer would render most public-key encryption architectures—used for applications from banking and credit cards to the power grid—obsolete. They rely on numbers too big for conventional computers to factorize, but which a quantum computer could.

Building quantum computers is a very heavy lift. They require hugely expensive infrastructure to stabilize the qubits at temperatures near absolute zero. They also generate high error rates, or "quantum noise," for which researchers have to compensate. Developers are probably years away from the large-scale code-breaking quantum computer everyone worries about—although once scientists and engineers start using quantum computers to build the next generation of quantum computers (since modeling complex systems like themselves is one of their strengths) the timeline could quickly shorten.

Beijing is America's chief quantum-computing rival. It spends at least $2.5 billion a year on research—more than 10 times what Washington spends—and has a massive quantum center in Hefei province. China aspires to develop the code-breaking "killer app," which means protecting U.S. data and networks from quantum intrusion is a vital security interest.

Congress enacted the National Quantum Initiative Act late last year, which commits an additional $1.25 billion over five years—still a fraction of China's effort. In addition to more money, the U.S. needs a three-phase national-security strategy to protect and defend American data, networks and infrastructure from future quantum attack.

First, dramatically increase efforts to develop encryption methods based on algorithms large and complex enough to foil quantum intrusion. The National Institute of Standards and Technology is working to set a comprehensive standard for these quantum-resistant algorithms so they can be deployed by 2024, but companies in the U.S., Canada and elsewhere are already building algorithms and other protective tools.

Second, use quantum technology itself to create the "unhackable" networks of the future. The same particles that make quantum computing possible can provide randomized and unhackable keys for encrypted transmissions, in the form of quantum random number generators and quantum key distribution, a method of securing information shared between two parties. Dismissed as a fantasy a few years ago, quantum cryptography has spawned companies in the U.S., Switzerland, South Korea and Australia, which are deploying the first components of a new quantum-based information-technology infrastructure. Eventually this will include satellites using quantum keys to transmit encrypted data.

Here again China has moved quickly. It launched the world's first quantum satellite in 2016 and shocked the world by creating a quantum-encrypted intercontinental video link from space to a China-Austria study group in Vienna. China has also created a 1,263-mile ground link between Beijing and Shanghai using quantum-encrypted keys between relay stations, which offers an ultrasecure network for transmitting sensitive data, including for China's military and intelligence services.

Third, require that all U.S. data and networks, including future 5G technology, be made secure from quantum attack while devoting resources to build the hack-proof quantum communication networks of the future. That will require working with America's closest allies, several of which are making key breakthroughs in the same quantum and postquantum technologies.

Promoting such cooperation has been a core mission at the Quantum Alliance Initiative, which convened a consortium of companies and universities from the U.S. and allied countries to develop global standards for quantum random number generators and quantum key distribution late last year. But no one can do all this alone, not even Google plus IBM plus Microsoft and the other big companies working in quantum computing. Leadership from the federal government is more imperative than ever. Google's breakthrough proves that the threats, as well as the opportunities, of quantum technology are real—and that quantum is poised to become the national-security issue of the 21st century.