**2AC**

**Innovation DA---2AC**

**Transparency over collective defense key to enable operational planning**

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

NATOs cyber-resilience experienced in crisis management and communication

Societal security, an emerging phenomenon in the field of strategy and security, requires **good** crisis management skills but also **communication** effectiveness in both the real and virtual worlds. **Business continuity** at NATO requires as foresaid the Alliance, to be resilient and surely for the purposes of this research paper, the Alliance and allies to be or become cyber-resilient.

By methodological approach, societal vulnerability continues and will always continue to exist, so far and as long as threats are there. Considering the current civil need to be always preparing for a new “cold era,” among others, considering the unlawful annexation by Russia of Crimea in 2014 (BBC, 2014) and following the disintegrating relations of NATO due to the unlawful act of Russia to Ukraine, the establishment of the USA and then taken over by NATO, of the Missile installation in Romania (Reuters, 2016) and the immediate reaction and accusation of Russia in regard to these developments (New York Times, 2016), the refugee challenges as an outcome on the constant fight against ISIS (US Homeland Security Committee, 2015), but also the phenomenal changes in the financial world (i.e., The Panama Papers (The International Consortium of Investigative Journalists (ICJ), 2016)), NATO is required to become truly resilient NATO, as should also nations and leaders.

All aforementioned elements are crisis management factors. NATO provides the **tools** and **method**ologie**s**, in which the Alliance is requested to reply strategically and operationally. To mitigating plans for pre-crisis, during crisis and after crises situations. For and during operations, logistics of deployment or information gathering and or training purposes, among others.

In such similar cases, the **legal** and **political perspectives** also on **cyber** operations should be **clear**. The **success** of an operation lays to **effective logistical** and **operational support**. Therefore, the legal aspects that come with **sharing** of **info**rmation, on how to **deploy forces**, identify **key threats** and elements in cyber-space, are **important**. The Internet has no borders. And threats can easily infiltrate the national e-space and boundaries. Leaders are welcomed upon to take strong strategic-led decisions.

NATO is to ensure protection of all infrastructure. The Allies should be able to **anticipate**, **identify**, **mitigate**, and **recover** from “hybrid attacks (NATO Review, 2016)”—the dimension(s) of simultaneous attacks, while reducing the threat of destabilization and or spreading fear.

In a civic society, it is our **responsibility** to ensure adequate **awareness** on cyber-defense and security. To **learn** about the **necessity** to protect all infrastructures, **NATO’s collective defense should be characterized by** **burden sharing**, **openness**, flexibility, and **transparency** in cooperation and **info**rmation **flow** among **member** state**s**. Through **preparedness**, strategic and operational awareness, **strategic resilience can be achieved**. Response time and framework will then allow NATO to counter threats as they emerge.

**BUT, tech investment without clarifying article 5 first causes offensive ops---those escalate and turn the DA**

Sophie **Arts 18,** program coordinator supporting The German Marshall Fund of the United States’ (GMF) security and defense policy work in Washington DC., “Offense as the New Defense: New Life for NATO’s Cyber Policy,” GMF Policy Brief No. 039, 2018, https://www.gmfus.org/publications/offense-new-defense-new-life-natos-cyber-policy

Against the backdrop of a fast-developing **cyber threat landscape**, NATO has **struggled** to enact a **comprehensive strategy** that **sufficiently prepares allies** to **deter** or **defend** themselves against **cyberattacks**. While important steps have been taken, the alliance is still nowhere near ready to face cyber threats at the ‘speed of relevance’. **Individual members’** guarantees to use their **cyber capabilities** on behalf of the alliance – as the United States announced this year – can help fill that gap in strategy.

**Yet**, without a **well-defined** **policy agreement** between the member states and a clear command structure in overseeing NATO operations, this approach **risks unintended consequences** – particularly as **offensive cyber operations** have the potential of **cascading** into **conventional conflict.** To **prevent** such a scenario, allies should further **formalize** their **cyber strategy** through top-down **guidance** and **increase** their **cooperation** with partners to broaden their spectrum of potential responses. **Most importantly**, NATO needs to **streamline** its **decision-making process** in the cyber domain and to **define** potential **response scenarios** – including and short of evoking the collective-defense clause **under Article 5.**

**Grand is about ambiguity in respect to adversaries actions---ie allies need to accept that hybrid warfare involves ambiguity and plan for contingencies, which IS the AFF**

**The AFF maintains strategic ambiguity with respect to responses but sets clear red lines for thresholds which solves the DA AND avoids miscalc**

Charlie **Dunlap 16**, former deputy judge advocate general of the United States Air Force, joined the Duke Law faculty in July 2010 where he is a professor of the practice of law and Executive Director of the Center on Law, Ethics and National Security, ““Cybervandalism” or “Digital act of war”? America’s muddled approach to cyber incidents won’t deter more crises,” Lawfire, 10/30/16, https://sites.duke.edu/lawfire/2016/10/30/cybervandalism-or-digital-act-of-war-americas-muddled-approach-to-cyber-incidents-wont-deter-more-crises/

What to do? Develop norms as to the “red lines”

It is vitally important, however, to appreciate that simply because a particular cyber act may **legally constitute** an “armed attack” that might **qualify** for the political characterization of an “act of war,” that doesn’t mean that a country is **obliged to respond** to it with force. Indeed, there are many political reasons that would counsel against doing so. This is where Mr. Painter goes wrong with his discussion about “strategic ambiguity.”

In deterrence, **ambiguity** may be **useful** with respect to a **response**, but it is **markedly less so** when you are talking about the **threshold**. **Misunderstandings** as to where the proverbial “**red lines**” are set can lead to **dangerous miscalculation**, **unintended escalation**, and **unwanted conflict**. Given the **enormous potential** of cyber acts to do harm, potential actors ought not to get **mixed messages** as to how the U.S. considers **harmful cyber activities.**

Frustrations with the **opaqueness** as what cyber activity would constitute a casus belli appears to have motivated Congressman Mike Rounds to propose a bill earlier this year that would require the President to develop a policy for determining “when an action carried out in cyberspace constitutes an act of war against the U.S.”

Rounds points to testimony of Marine Lt. Gen. Vincent Stewart, director of the Defense Intelligence Agency, as part of his rational for the legislation. Stewart admitted that a “much fuller definition of the range of things that occur in cyber space [is needed], and then [we should] start thinking about the threshold where an attack is catastrophic enough or destructive enough that we define it as an act of war, I think that would be extremely helpful.”

Stewart isn’t alone in not “fully” understanding where the threshold lies. Other **Pentagon leaders** apparently are equally **uncertain**, something that raises the obvious question: **if our leaders don’t know**, how can we expect **potential adversaries** to understand which acts might **spark a full-blown war?** At the same time, except in the most aggravated cases, enumerating **in advance** precisely which cyber acts exceed the use of force threshold might be nearly impossible.

This is where **norm development** in international law comes into play. In doing so, the U.S. needs to use the language of international law. Political terms like “digital acts of war” are unhelpful not only because they do not track with the language of the law, they also can imply to the general public a level of response that is unnecessarily provocative and even inconsistent with the proportionality and necessity factors intrinsic to a lawful exercise of self-defense, especially in the complex cyber arena.

**Innovation is stalling.**

Christopher **Cole 21**, partner at Crowell Moring, “Lawmakers Worry Rampant Mergers Crushing US Innovation,” Law360, lexis.

**Innovation** across the U.S. economy has suffered as **antitrust laws fall short** in **stopping** predatory **merger deals** and enforcers allow **massive industry consolidation** to continue **unabated**, **experts said** **Wednesday** on Capitol Hill.

In the **latest congressional hearing** focused on **possible overhauls** of **American competition laws** to deal with **industry concentration** in sectors ranging from **technology** to **pharmaceuticals**, **real estate** and **agriculture**, a Senate panel zeroed in on the impact of monopolies on the development of cutting-edge products and services.

Antitrust **advocates** and **business figures** **testified** that the U.S. economy faces a **growing threat** from **large companies'** **m**erger and **a**cquisition strategies that aim to **knock out startups** and growing **rivals**, then **take advantage** of **market power** to continue **profiting off old technologies**. The trend **stifles U.S. innovation** and **harms consumers**, they said.

Senators looked to the experts to inform the lawmakers' biggest push in years to revamp antitrust laws, including a major bipartisan bill introduced in October, the American Innovation and Choice Online Act. The bill would make it harder for online sales platforms to self-preference their own products. Sens. Amy Klobuchar, D-Minn., and Chuck Grassley, R-Iowa, are lead sponsors of the bill, one of numerous antitrust proposals circulating on Capitol Hill.

"It's always been innovation that has fueled the American economy," said Klobuchar, who chairs the Senate Judiciary antitrust panel, but that "cannot thrive without open and competitive markets."

Monopoly power is on the increase in industries "from cat food to caskets," Klobuchar said, and that **stifles** the ability of **new companies** that may develop **better products** or **services** to **gain funding** and **enter the market competitively**. "We also have to remember that **innovation is all about competition**," she said.

Utah Sen. Mike Lee, the ranking Republican on the subcommittee, also voiced concern about consolidation suffocating the economy. Lee said that "I'm a huge advocate of the consumer welfare standard" that federal courts use to assess whether market behavior is unlawfully anticompetitive but "when competition suffers, so does innovation."

"One might say that competition is itself the mother of innovation," said Lee, who has been working closely with Klobuchar and Grassley, the full committee's ranking Republican, on antitrust legislation this year.

Still, Lee said lawmakers and enforcers must take care not to carry out "regulatory overreach" that ends up protecting no one except market incumbents when they make it harder for startups to succeed. Lee touted Utah's "pro-free market" approach that he said has been a magnet for new businesses and driven the quality of life higher in the Beehive State. "I do worry, however, that D.C. bureaucrats may spoil the party for everyone," he said.

Conservatives also voiced concern that consolidation of power in Big Tech has allowed the top companies to rein in free speech, and Lee pointed to the controversy over the startup social media platform Parler, which almost sunk amid the turmoil over the 2020 election.

The vast technology sector was only one aspect of Wednesday's hearing, however, as several witnesses talked about growing monopolies in pharma, real estate and other parts of the economy where they said behemoths' market power was holding back innovation.

Diana Moss, president of American Antitrust Institute, told senators there are many reasons that innovation is currently struggling in the U.S. economy. She said the financial markets' "laser focus on shareholder returns" based on the bottom line and short-term profits was making it more difficult for companies to invest in much-needed research and development.

"Another reason is weaker antitrust enforcement over the last 40 years," Moss said.

Alex Harman, competition policy advocate at Public Citizen, the liberal-leaning advocacy group, called unfettered merger and acquisition activity and the massive buildup of a small number of companies "one of the most critical issues of our time." Harman said there had been an "**alarming increase** in **consolidation** throughout the economy."

Another witness, Roger Alford, a professor at Notre Dame Law School, identified **multiple competitive problems** rippling through the economy. One of the sectors **hard-hit** by a resulting **lack of innovation** is real estate sales, said Alford, a former deputy assistant attorney general with the U.S. Department of Justice Antitrust Division.

**Innovation DA---AT: China Impact**

**AFF solves Chinese hybrid threat by contingency planning---that’s key to security**

Lauren **Speranza 20**, director for trans-Atlantic defense and security at the Center for European Policy Analysis, 7/8/20, “China Is NATO’s New Problem,” https://foreignpolicy.com/2020/07/08/china-nato-hybrid-threats-europe-cyber/

Over the past decade, Chinese companies have invested billions of dollars throughout Europe—buying up **critical infrastructure** and increasing Beijing’s **political clout** across the continent. As Chinese firms, often with strong ties to the state and Chinese Communist Party (CCP), acquire parts of sensitive ports, pipelines, and telecommunication networks, China’s incursions into Europe’s security umbrella are drawing serious concern.

But **NATO**, long worried about Russia, has largely been silent on China. **Now**, that is changing. NATO Secretary-General Jens Stoltenberg recently called on the alliance to stand up to Beijing’s “bullying and coercion,” underscoring how China’s rise is fundamentally shifting the global balance of power. **It’s apparent** that NATO can **no longer ignore the threat**. If the alliance hopes to **remain competitive**, it will need to develop a **new strategy** for dealing with Beijing.

First, NATO needs a **common assessment of China’s hybrid threats**—a mix of diplomatic, economic, security, information, and technological actions designed to quietly **undermine democratic states and institutions** to Beijing’s benefit while avoiding a traditional conflict. While China’s conventional military threat in the Indo-Pacific is far from NATO’s borders, its hybrid activities are happening in the alliance’s own backyard.

**Cyber-espionage**, **i**ntellectual **p**roperty **theft**, **infiltration of critical infrastructure**, **debt manipulation**, and **disinformation** are prime examples. While these threats may **seem** to fall outside of NATO’s purview, they pose serious security risks for the alliance. For instance, China’s desire to invest in Lithuania’s Klaipeda Port may not look like a problem for NATO on its surface. But its investments have worrying strings attached that give China operating control over the infrastructure. That control could decrease **allies’ willingness to move military forces**—**including sensitive technologies**—through the port and its surrounding networks. This could lead to disrupted planning and fewer military exercises, decreasing NATO’s ability to defend the Baltic States during a crisis with Russia. This could also open the door for **pragmatic collaboration between China and Russia** to undermine trans-Atlantic security.

Allies need to forge a **shared understanding** of these risks through **information-sharing and dialogue**—no small feat for countries that do not see eye to eye on China. Some are even willing to ignore such vulnerabilities, due to economic benefits or disenchantment with trans-Atlantic institutions. The **U**nited **S**tates has a **critical role** to play in getting allies **on the same page** and **setting common goals** for countering China’s hybrid activities.

Second, NATO needs to focus on public diplomacy. **NATO** has an important role to play in the battle against the CCP’s global narratives, which Beijing promulgates through **hybrid activities**. To defend the trans-Atlantic values on which the alliance is built—freedom, **democracy**, **rule of law**, and **human rights**—NATO should clearly communicate China’s violations of these principles and its propaganda efforts to cover them up. (These include, among others, human rights abuses against ethnic Uighurs in Xinjiang and violations of the U.N. Convention on the Law of the Sea in the South China Sea.) NATO should also enhance its outreach to key partners in the Indo-Pacific, such as Australia, Japan, New Zealand, and South Korea, which can serve as important counterweights to Chinese influence in the region. Effective public messaging also means getting serious about attributing the blame for attacks, as the European Commission recently did over Chinese disinformation around COVID-19, to raise the pressure on Chinese officials. Trans-Atlantic countries have **struggled to shape China’s behavior** because they cannot prove malign intent or agree to call out Beijing for its subversive efforts. Allies should develop **clearer guidelines**—**what needs to be proved**, **by whom**, **and to what degree**—to enable **collective attribution**. NATO is strongest when it speaks with one voice. It should use that voice to demand transparency and change from China.

Third, the alliance should step up its counteroffensive. China’s hybrid actions intentionally **blur the lines** between what is **legally permissible**, **politically inappropriate**, and **downright escalatory**.

This makes it difficult for leaders to determine **appropriate responses**, producing a reactionary approach **thus far**. But an intensifying geostrategic competition has already begun. To compete in this environment, the trans-Atlantic community needs a **more proactive approach**. Rather than waiting for China to invest in the next major European port, allies should coordinate legislation to prevent the riskiest Chinese acquisitions. And rather than waiting for more Chinese cyberintrusions, allies should collaborate on responsible, targeted offensive cyberactions. Over time, this would help **dissuade China** from manipulating investments in critical infrastructure, conducting cyber-espionage, and other hybrid activities. While adopting a more offensive posture remains controversial among certain allies, it is **gaining traction across Europe** and is **strongly supported in Washington**. Although NATO, **as a defensive alliance**, should not implement such a counteroffensive, policymakers should **leverage it** as the **primary forum** to **coordinate actions among willing nations**.

Fourth, NATO needs to deepen its cooperation with other key players, such as the European Union and the private sector. Where NATO lacks the mandate and means, the EU and multinational businesses play critical roles in developing, implementing, and enforcing the legislation and financial incentives necessary to counter Chinese hybrid threats. Complementary to that, NATO and its allies can focus on providing intelligence, defending cyberspace, developing capability targets for new technologies, conducting exercises and **contingency planning**, informing resilience requirements for secure infrastructure, and bolstering deterrence. Despite the political obstacles that impede more formal NATO-EU cooperation, allies should look to the European Centre of Excellence for Countering Hybrid Threats in Helsinki to bring together NATO and EU staff, national officials, and industry voices in one place to align their counter-hybrid policies for China.

The Chinese government’s manipulative efforts around the coronavirus have thrust China’s hybrid activities to the center of trans-Atlantic debates. Policymakers need to **seize the moment** and respond by **“using NATO more politically,”** in Stoltenberg’s words. NATO is first and foremost about its nations. In the fight against China’s hybrid threats, these nations bring much more to the table than military power alone. They have access to a broad range of tools—military, political, economic, technological, and information—which the alliance can use to its collective geopolitical advantage in the competition with China. What NATO needs now is a strategy to leverage those tools in a **coordinated manner**. That will go a long way in solving NATO’s China problem.

**Russian success spurs Chinese aggression---we solve best**

Sascha Dominik (Dov) **Bachmann et al 19**, Professor, Canberra Law School, “Competition short of war – how Russia’s **hybrid** and **grey-zone** warfare are a **blueprint** for **China’s global power ambitions** ,” Australian Journal of Defence and Strategic Studies Vol. 1 No. 1, November 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3483981

China’s territorial ambitions as a ‘hybrid threat’?

China has participated in **more territorial disputes** than **any other state** since the end of the Second World War.40 Many of these disputes could be considered **expansionism**, with the exception of Taiwan, which has remained a reunification objective of the People’s Republic of China (PRC) since 1949. The disputes include **land border claims** and counter-claims, such as with **India**, and arguments with **Hong Kong** over its **separate legal system** are also increasingly a **source of tension**. However, the primary focus of Chinese expansionism tends to be in the **maritime environment** with disputes over the Paracel and Spratly Islands in the **South China Sea** and the **Senkaku Islands** in the **East China Sea.**

The Chinese maritime disputes especially in the South China Sea are **complex**, involving multiple overlapping claims with other regional states but also with other stakeholders who seek peaceful resolution of claims and assurance of freedom of navigation. The establishment of military facilities on the islands, in breach of a ruling of its claim by The Hague, **exacerbated the situation**, leading US and other navies to conduct regular freedom of navigation exercises through the South China Sea.

In addition to China’s ambitions associated with territory in its direct proximity, China has developed a strategy for its future economy with the Belt and Road Initiative. Critics of this strategy assert that the associated infrastructure elements of the initiative are essentially an alternative means of securing key overseas territory, or a new form of colonialism.41 An obvious example of this strategy is China’s effective acquisition of the port of Hambantota in Sri Lanka.42

China’s approach to its territorial claims is one in which changes are implemented **incrementally** and thereafter **become the new normal**. Occupation of South China Sea islands is an example, in which China’s 2019 Defence White Paper **characterises** international **freedom of navigation** as ‘countries from outside the region… **illegally** entering **China’s territorial waters**… **undermining China’s national security’**.43

In a 2010 article, Fravel asserted that China was unlikely to resort to armed conflict or even aggressive expansionism in pursuing their territorial claims. 44 **However**, since that publication, we have seen examples in the East and South China Seas in which **aggression** has been **clear**, with challenges between **military platforms** and with conflict often **narrowly averted.**

Despite these tensions and occasional incidents, China’s conduct of expansionism in the South China Sea primarily has been in the **grey-zone**, in that each step has been **calculated** to **achieve objectives** **without crossing a threshold of** **warfare**. However, can we consider it to be hybrid warfare? That is, has the posturing of forces been complemented by other activities to achieve their goals? Hoffman regards China as being ‘well organized to conduct operations short of military conflict’45 utilising three forms of nonwarfare, namely noncontact (fei jierong), nonlinear (fei xianshi) and nonsymmetric (fei duicheng)’.46

Such influence activities are widely suspected to be behind the Philippines government’s softening of their stance against China in relation to the South China Seas dispute.47 Such influence may be overtly undertaken through incentives such as Belt and Road Initiative agreements, although there is evidence that such initiatives can have a covert element and take advantage of corrupt regimes.48 Influence can extend to attempted corruption of Western politicians to advocate for Chinese policies over the dispute.49 China more broadly exerts influence through a combination of political warfare activities, including mobilisation of diasporas, tasking of students, financial assistance to individuals and institutions, economic manipulation and large-scale cyber and other information operations.50

Hybrid Lawfare – exploiting the legal grey-zone of modern conflict

Hybrid warfare is an open concept with different elements. Lawfare, for example, is a new aspect of non-kinetic conflict aiming at ‘using law as a weapon to manipulate legal paradigms’.51

Lawfare is being used by **Russia** and **China** (in the context of the South China Sea as discussed in this article) both within and outside the scope of traditional armed conflict. For Russia the use of lawfare is ‘a continuation of its policy of using every tool at its disposal to achieve its political and geo-strategic goals’52 and a ‘force multiplier’ to meet its political, military and legal objectives, as highlighted in its Military Doctrine of 2014 and its National Security Strategy of 2015.

Both China and Russia have been active in the **use** and **abuse** of the **rule of law** in order to either **prepare military action** or to **justify it** **after completion** of the mission. Russian justification of the occupation and then subsequent annexation of Crimea is an example of the latter; while the Chinese justification for its claims over the South China Sea is an example of the preparation of a legal basis for the potential use of force in self-defence when protecting own sovereign rights and (island-) territory.

Lawfare in conjunction with hybrid warfare ‘provides a **layer of “fake” legitimacy**, or at least reduces the erosion of **apparent legitimacy**, due to the **nonattributable aspects** inherent in hybrid warfare while using “easy” hybrid warfare methods’.53 Lawfare can be used as a method of hybrid warfare or influence operations.54 US writer, Kittrie came up with the following test: (1) the actor uses law to create the same or similar effects as those traditionally sought from conventional kinetic military actions—including impacting the key armed forces decision-making and capabilities of the target; and (2) one of the actor’s motivations is to weaken or destroy an adversary against which the lawfare is being deployed.55

Russia’s use of lawfare in Ukraine thus exploits both (1) the undefined definition of the conflict as aggression and (2) the unwillingness of the international community to label it as such. And, it maintains uncertainty through a strategic (dis)information campaign which keeps the nature of the conflict open, so it is unclear whether it is international armed conflict, non-international armed conflict or civil unrest.56 Here clear parallels regarding China’s actions in the South China Sea can be drawn.

China and Russia’s use of the ‘weaponisation’ of the maritime environment as grey-zone tactics or consolidation of a hybrid warfare based approach

We are now turning to the example for such a lawfare approach: the so-called weaponising of the maritime environment through terraforming as part of a multifaceted security strategy. China’s Defence Minister, Wei Fenghe, argued in 2018 that, ‘The islands in the South China Sea have long been China’s territory. They’re the legacy of our ancestors and we can’t afford to lose a single inch of them’.57

Officially, China claims that its overall intention was to use the extension of its territorial waters peacefully and to serve solely its commercial needs. This is **doubtful**, given that China has **actively weaponised** the **claimed territories**. Sumihiko Kawamura, a former rear admiral and commander of Japan’s Maritime Self-Defence Force’s antisubmarine air wing, suspects that China wants to use the South China Sea as leverage against the US Pacific security projection. Kawamura believes Beijing is trying to turn the South China Sea into ‘a **safe haven’** for its **nuclear-powered submarines**, which are **armed with ballistic missiles** that can reach the United States. 58

In this context, it is worthwhile to note that China did **lose its case** for claiming the SCS waters in a 2015 case brought before the UN Permanent Court of Arbitration by one of the affected states, the Philippines. China therefore failed spectacularly with its attempt to successfully use lawfare by manipulating the provisions of the United Nations Convention on the Law of the Sea to argue own sovereign rights (like exclusive economic and fishing rights) over the majority of the SCS waterways.59 China later decided to **ignore the ruling** and to **consolidate its illegal position** further by **illegally maintaining**, and even **expanding**, so-called **E**xclusive **E**conomic **Z**one**s** in the disputed SCS waters.60 This consolidation manifests itself in Chinese **below the threshold** **grey-zone tactics** like **policing** its falsely claimed territorial waters around **artificially built islands**, **interference** in **air-traffic** and **challenging US and allied navies** in their rightful freedom of seas navigation patrols, to name just a few examples.61 China has created, like Russia in respect to the illegally annexed Crimea, **a fait accompli.**

In Russia’s case, immediately following the annexation of Crimea in 2014, Russia began the planning and construction of the Crimean Bridge over the Kerch Strait in Ukraine to support its territorial claims. The project was successfully completed in May 2018 as the so-called Unification Bridge and was followed subsequently by Russian military action to ensure regional observance of the new status quo.62 Russian naval units attacked and boarded three Ukrainian vessels in autumn 2018 for having allegedly violated Russian territorial waters when passing through the Kerch Strait.63 What became known as the ‘Kerch Strait’ incident was followed by the effective closure of a part of the Sea of Azov waterway whenever Russia decided to conduct live fire naval exercise,64 thus violating Ukrainian territorial waters, as the annexation of Crimea was and continues to be regarded as illegal.65

Russia’s actions can be seen as consolidation action of its gains from its successful hybrid warfare campaign against the Ukrainian state when seizing Crimea. With the annexation complete and little to fear in terms of military action or meaningful sanctions, Russia can now resort to the use of traditional hard power in consolidating and protecting its position.

Both China and Russia have provided examples of how territorial gains made through hybrid warfare and grey-zone tactics can be weaponised further to serve wider national security aims and ambitions by warranting the question of how to respond in an effective manner.

Russian warfighting stratagems as **dangerous precedent**

The question arises of what is new in Russian warfare since 2008. Among a host of features of the new war some are indeed noteworthy: the non-declaration of war, the use of armed civilians, non-contact clashes like the blockade of military installations by ‘protestors’, the use of asymmetric and indirect methods, simultaneous battle on land, air, sea, and in the informational space, and the management of troops in a unified informational sphere.66

The authors have written extensively about hybrid warfare and its Russian equivalent as reflexive control67 and nonlinear warfare. Russian Hybrid Warfare has become known as the so-called ‘Gerasimov’ doctrine68— though while Western military authors (including us) continue to use this reference, it is at least questionable if General Gerasimov actually intended to have his thoughts and reflections on evolving Russian military operational approaches be regarded as a military ‘doctrine’ in a strict sense.69 So, while the existence of such a doctrine is debatable, the overall success of contemporary Russian warfighting is not, and the term hybrid warfare is a good characterisation of Russia’s contemporary aggressive foreign policy.

The actual **consequences** of Russia’s hybrid warfare are **far-reaching**. Russia’s foreign policy (and also China’s) of assertive **nationalist posturing**, **meddling** in internal affairs, **political warfare**, and **hybrid warfare** disrupt the Western narrative of **globalisation**, **rule of law**, **democracy** and **interconnectivity**. This creates an **untenable situation** where the West is responding to **ad hoc threats** in an **increasingly less assertive way** instead of **defining** and **implementing** a joint foreign policy that would **deter** such an adversary.

Russia’s version of hybrid warfare, whether we refer to it as Gerasimov’s doctrine, Russian Hybrid Warfare or reflective control, has been **successful**. Firstly, Russia proved successfully ‘that this warfare not only includes nonstate actors but also states’.70 Secondly, it proved the effectiveness of this form of warfare because Russia’s departure from its reliance on kinetic resources also reduced the need for using **conventional military power** in a **conventional sense**, which **benefits** the ‘**weaker’** opponent. And thirdly, hybrid warfare as part of a **wider** **information-operation** and **lawfare** approach provided **false legitimacy** due to **attribution questions** and the **potential for denial** by the target state for political reasons. This **Russian success** with hybrid warfare is what China seems to be **emulating** in respect to its current territorial expansion: the use **of ‘little blue men’**, **information operations**, economic and diplomatic **pressure** and **lawfare** (which albeit failed).

**Innovation DA---UQ**

**US total factor productivity has been abysmal since the 70s.**

Alexander **Kersten 21**, Deputy Director and Fellow, Renewing American Innovation Project, “Why Renewing American Innovation? The “Endless Frontier Act” and Biden’s Bid for Maintaining U.S. Global Competitiveness,” CSIS, https://www.csis.org/analysis/why-renewing-american-innovation-endless-frontier-act-and-bidens-bid-maintaining-us-global

Despite **Silicon Valley** and the millennial generation’s **supposed penchant** for **innovative disruption**, U.S. **total factor productivity** has been **slowing** since the **1970s**. **Productivity toda**y is the **lowest** in more than a **century**. Innovation, historically a clear driver of U.S. productivity, means the creation of ideas and inventions that are translated into practical value and improve the quality of people’s lives directly or via their ability to grow the economy. Whether measured in terms of triadic patents (patents filed in the United States, Europe, and Japan), most available measures of productivity, or even startup company creation, the United States’ **trademark innovative spirit** has been **gradually dampening** for **decades**. And if not for **China’s meteoric rise** this century, the United States might **still be sleepwalking**—optimistically but without a serious plan—instead of waking up to the need for a coherent national strategy.

U.S. Complacency, and How We Got There

Noted George Mason University economist Tyler Cowen and other experts have recognized a growing “**complacency**” in American life as the indicator of a **societal shift** from the United States’ **early dynamism**. From the turn of the twentieth century until roughly the moon landing of 1969, the breakneck pace of groundbreaking technologies that directly affected the quality of life and the structure of U.S. society was simply astounding. Yet, since the first moon landing in 1969, **only** the **internet** and its **application** to more and more parts of our lives can claim to have made any **meaningful impact**—meaning that physically the world of 1969 is much more like that of 2021 than 1969 was of the early twentieth century. This, of course, is not meant to discredit the great advances in medicine and human genomics made in the last few decades, for example, but to show how the **rate** of **society-changing innovations** has **not** **maintained** the **pace** that existed from the **mid-nineteenth century** until roughly 1969.

In the developed world, this slowdown has unfortunately contributed to **wage stagnation**, the **shrinking** of the **middle class**, and **greater political polarization** domestically. **Coinciding** with the **waning** days of the **Soviet Union’s power** in the 1980s, the U.S. **innovation decline** was **masked** at home. Further, the Soviets of that period no longer posed a technological threat to the United States. Japan on the other hand, posed a great technological threat in the 1980s but was and is a staunch U.S. ally, and not a security threat. Unchallenged abroad and riding the dual-edged optimism of the internet boom of the 1990s and the victory over communism, the United States missed the ways in which it was giving up the advantages that made it such a powerhouse in the mid-twentieth century.

**US manufacturing and high-tech innovation are both in deep decline.**

Robert D. **Atkinson 20**, PhD, founder and president of ITIF, “How Nine Flawed Policy Concepts Hinder the United States From Adopting the Advanced-Industry Strategy It Needs,” ITIF, 8/10/20, https://itif.org/publications/2020/08/10/how-nine-flawed-policy-concepts-hinder-united-states-adopting-advanced

THE CASE FOR ACTION

Before describing the **chain of logic** that points directly to the **need** for an **advanced-industry strategy**, it’s important to lay out the **case** for some sort of action. In short: Over the **last two decades**, the **U.S. economy** has **lost its competitiveness edge**

Perhaps the **most obvious sign** of U.S. economic decline has been the **erosion** of the country’s **manufacturing base**. From 2001 to 2010, the United States lost **42,400 factories** (three-quarters of which employed at least 500 workers while in operation), 32 percent of its manufacturing jobs, and much of its technical edge.1

Since then there has been **further erosion**. From 2007 to 2019, while **GDP grew** by **22 percent**, **real manufacturing value-added** grew by just **5.6 percent**. As a result, manufacturing’s **share** of gross domestic product (**GDP**) **fell** from 13.2 percent to 11.4 percent. This also **obscures** **significant differences** **within industry sectors**. All of the eight nondurable goods sectors (such as paper, chemicals, and plastics) produced **less** in **absolute terms** in 2019 than they did in 2007. Moreover, as a number of analysts—including the Information Technology and Innovation Foundation (ITIF)—have shown, the Bureau of Economic Analysis (BEA) significantly overstated the output growth of the computer sector (NIACS 334) because it assumes that when a computer doubles in speed due to Moore’s Law, actual output also doubles. Leaving out the production of computers—most of which has moved overseas—U.S. manufacturing output actually declined by 3 percent.

Just as troubling is that U.S. manufacturing is in a **productivity slump**. In 15 out of 18 years from 1990 to 2007, **manufacturing productivity** grew **faster** than overall non-farm business productivity, often by more than twice as much. But between 2008 and 2019, manufacturing productivity grew faster in just **3** of the 12 years. In 2019, while business productivity grew 1.9 percent, manufacturing productivity grew just **0.1 percent.** One reason for this might be U.S. manufacturers increased capital expenditures by just 17 percent between 2008 and 2017 (the latest year for which data is available), or one-third the rate of the information sector (e.g., Internet, communications, etc.). Without robust productivity growth, manufacturing gets **less competitive globally**, which is why it grows **more slowly than GDP.**

One would think, with manufacturing productivity growing more slowly than the rest of the economy, job growth would be robust (and as other sectors become relatively more efficient). But at the end of 2019, manufacturing employment was still 6.5 percent below its pre-recession levels.

But even if America is losing manufacturing, surely it is still leading in **innovation**, **right?** **So goes the thinking** (as if manufacturing is not innovative). But on **many measures**, when **controlling** for the **size** of the **economy**—such as government and business research and development (R&D) expenditures and patenting—the United States is **no longer the leader**. It ranks **12th** in **patent cooperation treaty patents** filed as **share of GDP,** **23rd** in **researchers per capita**, **27th** in **high-tech exports** as share of trade, and **44th** in **scientific and technical articles** as a share of GDP.2 Moreover, in 2019, the United States ran an **all-time-high trade deficit** of $132 billion in **advanced technology products**, down from a $4.5 billion trade surplus in 2001.3 With China, the trade deficit in electronic products was $184 billion in 2017, as U.S. exports totaled just $21 billion.4

Also, many **once-iconic** U.S. **advanced-industry firms** have **lost** **significant global market share** or even **gone out of business**. Forbes issues a list of the **top 2,000 firms each year**. To be sure, from 2006 to 2019, a number of U.S. technology firms **increased** their **global ranks** significantly, particularly in software (e.g., Microsoft); semiconductors (e.g., Intel, Micron, and Nvidia); and Internet services (e.g., Facebook). **But** many **hardware** and **related firms** either **lost ground** or **went out of business**. **Once-global leaders** such as **Lucent**, **Motorola**, and **Nortel** (a Canadian firm that at one time employed thousands of U.S. workers) are now **defunct**. And leaders such as **IBM**, **Hewlett Packard**, **Agilent** (formerly part of HP), and **General Electric** all **fell significantly**. (See table 1.)

**China is out innovating the US in the SQUO**

Christopher **Darby &** Sarah **Sewall 21**, Christopher Darby, CEO of In-Q-Tel, National Security Venture Capital Arm, Sarah Sewall, Executive Vice President for Policy at In-Q-Tel. Formerly U.S. Undersecretary of State for Civilian Security, Democracy, and Human Rights, The Innovation Wars: America’s Eroding Technological Advantage, Foreign Affairs, https://www.foreignaffairs.com/articles/united-states/2021-02-10/technology-innovation-wars

THE CHINESE JUGGERNAUT

The **changes** in American **innovation** would matter less if the **world had remained unipolar**. Instead, they occurred **alongside the rise of a geopolitical** rival. Over the past two decades, China has evolved from a country that largely **steals and imitates** technology to one that now also **improves and even pioneers it**. This is **no accident**; it is the result of the state’s deliberate, long-term focus. China has invested massively in R & D, with its share of global technology spending growing from under five percent in 2000 to over 23 percent in 2020. If current trends continue, China is expected to overtake the United States in such spending by 2025.

Central to China’s drive has been a strategy of “military-civil fusion,” a coordinated effort to ensure cooperation between the private sector and the defense industry. At the national, provincial, and local levels, the state backs the efforts of military organizations, state-owned enterprises, and private companies and entrepreneurs. Support might come in the form of research grants, shared data, government-backed loans, or training programs. It might even be as simple as the provision of land or office space; the government is creating whole new cities dedicated solely to innovation.

China’s investment in **5G** technology shows how the **process works in practice**. Equipment for 5G makes up the **backbone of a country’s cellular network** infrastructure, and the Chinese company Huawei has emerged as a **world leader in engineering** and **selling it**—offering high-quality products at a lower price than its Finnish and South Korean competitors. The company has been buoyed by massive state support—by The Wall Street Journal’s count, some $75 billion in tax breaks, grants, loans, and discounts on land. Huawei has also benefited from China’s Belt and Road Initiative, which provides generous loans to countries and Chinese companies to finance infrastructure construction.

Massive **state investments** in **artificial intelligence** have also paid off. Chinese researchers now publish more **scientific papers** in that field than **American** ones do. Part of this success is the **result of funding**, but something else plays a big role: access to **enormous amounts of data**. Beijing has fueled the rise of **powerhouse companies** that sweep up endless information **about their users**. These include **Alibaba**, an e-commerce giant; **Tencent**, which developed the all-purpose WeChat app; **Baidu**, which began as a search engine but now offers a range of online products; **DJI**, which dominates the consumer drone market; and **SenseTime**, which provides facial recognition technology for China’s video surveillance network and is said to be the world’s most valuable artificial intelligence company. As a matter of law, these companies are required to cooperate with the state for intelligence purposes, a broad mandate that is almost certainly used to force companies to share data for many other reasons.

That information increasingly involves people living outside China. Chinese companies have woven a global web of data-gathering apps that collect foreigners’ private information about their finances, their search history, their location, and more. Those who make a mobile payment through a Chinese app, for example, could have their personal data routed through Shanghai and added to China’s growing trove of knowledge about foreign nationals. Such information no doubt makes it easier for the Chinese government to track, say, an indebted Western bureaucrat who could be convinced to spy for Beijing or a Tibetan activist who has taken refuge abroad.

China’s hunger for data extends to some of the most personal information imaginable: our own DNA. Since the COVID-19 pandemic began, **BGI**—a Chinese genome-sequencing company that began as a government-funded research group—has broken ground on some 50 **new laboratories** abroad designed to help governments **test for the virus**. China has legitimate reasons to build these labs, but it also has an ugly record of forcibly collecting DNA data from Tibetans and Uighurs as part of its efforts to monitor these minorities. Given that BGI runs China’s national library of genomics data, it is conceivable that through BGI testing, foreigners’ biological data might end up in that repository.

Indeed, China has shown great interest in biotechnology, even if it has yet to catch up to the United States. Combined with massive computing power and artificial intelligence, innovations in biotechnology could help solve some of humanity’s most vexing challenges, from disease and famine to energy production and climate change. Researchers have mastered the gene-editing tool CRISPR, allowing them to grow wheat that resists disease, and have managed to encode video in the DNA of bacteria, raising the possibility of a new, cost-effective method of data storage. Specialists in synthetic biology have invented a new way of producing nylon—with genetically engineered microorganisms instead of petrochemicals. The economic implications of the coming biotechnology revolution are staggering: the McKinsey Global Institute has estimated the value of biotechnology’s many potential applications at up to $4 trillion over the next ten to 20 years.

Like all powerful technologies, however, biotechnology has a dark side. It is not inconceivable, for example, that some malicious actor could create a biological weapon that targeted a specific ethnic group. On controversial questions—such as how much manipulation of the human genome is acceptable—countries will accept different degrees of risk in the name of progress and take different ethical positions. The country that leads biotechnology’s development will be the one that most profoundly shapes the norms and standards around its use. And there is reason to worry if that country is China. In 2018, the Chinese scientist He Jiankui genetically engineered the DNA of twin babies, prompting an international uproar. Beijing portrayed him as a rogue researcher and punished him. Yet the Chinese government’s disdain for human rights, coupled with its quest for technological supremacy, suggests that it could embrace a lax, even dangerous approach to bioethics.

THINKING BIGGER

**Washington** has monitored China’s technological progress through **a military lens**, worrying about how it contributes to Chinese **defense capabilities**. But the **challenge is much broader**. China’s push for **technological supremacy** is not simply aimed at **gaining a battlefield advantage**; Beijing is changing the **battlefield itself**. Although commercial technologies such as 5G, artificial intelligence, quantum computing, and biotechnology will undoubtedly have military applications, China envisions a world of **great-power** competition in which **no shots** need to be fired. Technological supremacy **promises the ability** to **dominate** the **civilian infrastructure** on which **others depend**, providing enormous **influence**. That is a **major motivation** behind Beijing’s support for **high-tech civilian infrastructure** exports. The countries buying Chinese systems may **think they are merely receiving** electric grids, health-care technology, or online payment systems, but in reality, they may also be placing critical national infrastructure and citizens’ data in Beijing’s hands. Such exports are China’s **Trojan horse.**

**Innovation DA---Link Turn**

**Article 5 clarification key to enable operational planning**

Piret **Pernik 14**, Researcher of Strategy Branch of the NATO CCDCOE, “Improving Cyber Security: NATO and the EU,” International Centre for Defence Studies, September 2014, https://icds.ee/wp-content/uploads/2010/02/Piret\_Pernik\_-\_Improving\_Cyber\_Security.pdf

Operational planning and **capabilities development**

A report by the defence committee of the UK parliament finds that NATO is **poorly prepared** to respond to the Russia’s use of asymmetric warfare, including cyber attacks, information and psychological operations. The committee urges the Alliance to develop its own asymmetrical warfare capabilities, discuss how to deal with these attacks and operations, and mount its own offensive operations.58 . It also calls NATO to **re-examine** the **legal** and **military** **doctrines**, **criteria**, and **responses** for the declaration and use of both Article 4 and **Article 5.**59 Likewise, James Stavridis, retired NATO's Supreme Allied Commander (SACEUR) believes NATO should stand up a cyber defence operations force under the SACEUR, as well as explore the utility of offensive cyber weapons.60 The need to integrate cyber into NATO’s military operations and operational planning has been acknowledged also by Jamie Shea.61 **Operational planning** both for **Article 5** and **non-Article 5 events** **along with** **capability development** must be adjusted to the reality of asymmetrical or hybrid warfare that employs a range of tools, including information operations and cyber attacks.

In addition to the need to integrate cyber into both military and civil emergency operational planning, NATO must improve the interoperability of cyber capabilities of the Allies and this process can be facilitated by the means that will be provided by the newly established NATO’s cyber range.

Furthermore, realistic **cyber threat scenarios**, as well as **clear** and tested **response procedures** and **mechanisms** should be in place. Operational **contingency plans** must **clarify** **which capabilities** NATO nations are **prepared** to **make available to the Alliance**, and the **mechanisms** for **collective assistance** by the individual Allies. A full range of response options (including kinetic means) accompanied by appropriate plans and capabilities need to be worked out. Since a simultaneous strike against NATO’s own and the member state’s infrastructure is likely, it would be prudent to ensure enough common capabilities to respond to both tasks. The existing two small RRTS consisting of a permanent core of six experts may be inadequate for simultaneous tasks.

In order to **enable** **military operational planning** NATO should consider the development of **cyber warfare doctrine**. It should establish a joint cyber command or headquarters (not unlike the Special Operations Headquarters), aligning joint strategy with political ends, at Supreme Headquarters Allied Powers Europe (SHAPE). Concerns about the legality of an offensive action in cyberspace aside, while NATO does not have an offensive cyber capability, member states’ capabilities could be used under Article 5 circumstances. NATO needs to ponder also what could be done to **help an Ally** experiencing a cyber attack causing serious damage to its private critical infrastructure.

**Setting a framework for cyber defense is also key to tech innovation**

Marios Panagiotis **Efthymiopoulos 19**, designated Dean and Associate Professor of International Security and Strategy of the College of Security and Global Studies, at the American University in the Emirates AUE, “A cyber-security framework for development, defense and innovation at NATO,” Journal of Innovation and Entrepreneurship (2019) 8:12, https://link.springer.com/content/pdf/10.1186/s13731-019-0105-z.pdf

Setting the stage

Cyber-security is yet to be **globally**, **legally**, **operationally**, and **strategically** **defined**. The scale of a security perspective is more attractive at this time considering the geostrategic challenges and threats. The possibility of **innovation** and **entrepreneurship** in the field is also a **tangible reality**, due to the necessary research and development methods. More so, the possibility of an open market economy sharing of knowledge and technological skills makes security and cyber-security or defense for that matter more attractive. What **lacks** in the world wide **legal** and **political** **framework of operations**, **exchange of information** and protectiveness from new sources or methods that can be deemed as elements of infiltration.

The article’s aim is to examine and recommend a global strategic framework for operational capacity and management resilience between allied and cooperative partners in the field of cyber-security. The current article is a follow up of prior scientific publications made in 2014 first and later in 2018, on NATO’s cyber-security strategy, presented through a framework of Cyber-Development, Cyber-Democracy, and Cyber-Defense (Carayannis, Campbell & Efthymiopoulos, 2014; Carayannis, Campbell & Efthymiopoulos, 2018). The aim is to converge diversified information on cyber-security, in a single strategic framework; reflect to the actual practical needs in understanding operations and tactical ability to deliver in multi-complex and dimensional world through management and operational efficiency capabilities. The article requests interoperability of aims and objectives under a global framework of cyber-security; through a strategic framework on cyber-security, global law can be proposed, defined, and adopted by the international community. The **strategic framework** will define **structures** that are needed to be put in place on a global scale, when reflecting issues of cyber-security and inclusive for **NATO**. It will define threats and challenges, as cyber-attacks are real. Cyber-security is not an asymmetrical or hybrid threat, but an **existential one.** Its destructive capacity can be multi-leveled and can also lead to human casualties. The future of e-safety lays at both a global estimation framework of what constitutes cyber-security and how we react to it; it lays in between cooperation of allies and members of wider alliances, against specified or approximate threats. Yet, its **framework** of aims and objectives, **management**, command and control, and operations will be defined and decided by **allied parties** only such as is the case of **NATO**.

**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.

The article’s design is based on cross-disciplinary and interdisciplinary approaches. It combines elements of global security and strategy, national and international law, economic development, and technological research and advancement and most importantly is innovative and entrepreneurial; its understanding will enable us to comprehend global and regional market establishment and convergence, as also economic changes. The setting of the study required lapse of time to showcase the need and the necessity of the subject. Current output reflects a set of written analyses, rules, and primary experiences. It methodologically acquired sources of information of related necessity and relevance, shaped the understanding, and need to point out for a framework of rules, regulations, management, and operations on cyber-security.

The article and its author frames a specific policy recommendation with regards to the creation of not only a regional alliance (NATO-based scale), Cyber-Security Strategy for the twenty-first century but a global one. The article defines the “dynamism” of cyber-security both as a topic and subject. Cyber-security is a twenty-first century element of policy orientation; a necessity for both collective and individual defense and security resilience.

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**

**Innovation DA---AT: Resilience Solves AFF**

**AFF key to resilience**

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

**Smart defense** and more so in the field of cyber-security is NATOs main priority policy. It does however reflect as well on to the tools and mechanisms used to innovated in and for management operations, processes, and tactics. It allows for defense entrepreneurial thinking and application. **Constant changes in strategy** and **policy** do request **efficient leadership** and **management** skills to operate. And so, should NATO’s cyber-resilience **strategic policy**.

Through a methodological period, such as in the NATO Summit in Brussels of July 2018, NATO will now have to show an enhanced progress report within the second quarter of 2019, assuring current and future abilities also in cyber-security, to counter current and emerging challenges in cyber-space. **Defense planning,** **operations**, and lessons learned are therefore a continued process that allows the **evolution of NATOs capabilities** which always need to be taken into account and more so in the field of cyber-security where the Cyberspace Operations Center will play a key role into it.

**Resilience** through smart and cooperative innovative defense **requires** NATOs **policy** on Cyber-defense to be also **effective**. As said, it requires **decision-making** and **leadership** in this policy context. In the framework of cyber-defense, NATO needs to **align** **supranationalized** national capability priorities and **standardize processes**, through **NATO processes.** In the framework of cyber-resilience at NATO, policies on standing management of operations need to be agreed upon. Therefore, **cooperative** and **consensus leveled agreements** need to come forth; NATO should produce a cost-effective projection planning and application for all operational exercise theaters reflecting the real yet also virtual worlds.

Cyber-resilience and methodological specialization through leaders’ policy decisions at the level of Heads of States and Governments in operational planning and practically applied are key components of and for success for the Alliance, considering threat assessments. Resilience with coordinated efforts may lower costs, fiscal, administrative, and human, but will **require** **developed technology infrastructure**. It will guarantee national engagement of states to NATO policies, when correctly pointed out. Let us not forget that **specialization** as a key national policy is and will always remain a form of **national interests**, which examined changing variables based on geographical interests, strategic sharing of costs, technological information, and intelligence sharing or operating in regional or global environments.