Research Division
NATO Defense College

NDC POLICY BRIEF
No. 19 – November 2020

The interstate conflict potential of the information domain

Dumitru Minzarari *

The coronavirus pandemic has not only triggered a crisis in public health and safety that engendered a significant economic fallout. The pandemic has also triggered an infodemic,[1] one that sets the context for a significant spike in anti-NATO[2] and anti-Western[3] propaganda. Unless countermeasures are taken, the already deteriorating public opinion *vis-à-vis* the Alliance can be expected to worsen.[4] Viewed individually, these two pandemic's outcomes have not critically threatened the Alliance; however, their combined effect could become a formidable challenge for NATO.[5] Despite the measures taken, the pandemic is likely to continue exacerbating the frustrations among member states, further fraying the Alliance's unity. This, arguably, is the most immediate and concerning challenge facing NATO today.

There is an acute realization within NATO that the Alliance must adapt and evolve to better understand and respond to emerging challenges. The Secretary General's efforts in launching a reflection process under the NATO 2030 initiative is a timely measure. But is its focus – becoming stronger militarily, stronger politically, and more global – the most efficient response?

This analysis claims that given the emergence of the information space as a new operational domain of war, the largest and most urgent challenge facing NATO is not the lack of military capabilities to deter or respond to possible aggressors. It is the weakened and shakier foundation of the political resolve required to mobilize the Allies' military capabilities against such aggressors. NATO's challengers do not question the technical ability of the Alliance to defend the interests of its member states. They question NATO's resolve to do it. And they actively target this resolve with the express aim of eroding it.

To respond effectively, there is a need to reconsider the organization's priorities and focus. During most of its history, NATO has had one main audience – its various opponents – which it sought to deter by convincing them of the Alliance's readiness and decisiveness for a military response against any aggressive behaviour or threat. Today, NATO ought to engage two more audience groups – the national governments and voters of its own member states – to convince them of the necessity of the Alliance. Failing to do this would risk leaving NATO's challengers to target and influence, without restraint, the behaviour of these groups.

* D. Minzarari was a Partnership for Peace Fellow at the NDC between March and July 2020, and a Visiting Scholar in September 2020. Starting October 2020 he is a Research Associate at the SWP, Berlin.

1 "The COVID-19 Infodemic", Editorial, *The Lancet Infectious Diseases*, Vol.20, Iss. 8, July 2020.

2 "Russia pushing Coronavirus lies as part of anti-NATO influence ops in Europe", *Defense One*, 26 March 2020.

3 Data shows a decreasing trend in support for NATO. See "Moscow's Coronavirus Offensive", *Politico*, 21 April 2020.

4 "Confidence in NATO in sharp decline", *Financial Times*, 10 February 2020.

5 Their impact is augmented by the exploitation of the coronavirus-related physiological and safety needs. They included efforts at increasing the number of infected by convincing the population that coronavirus was no more dangerous than the flu, leading to higher pressure on national health systems; at fueling tensions among citizens but also between the citizens and government (domestic politics mechanism); as well as efforts to blame coronavirus spread on NATO exercises (i.e. in the Baltic states), on Allies' stationed forces, or on the alleged artificial nature of the virus (the autonomy-security mechanism). See "EU Monitors Say Pro-Kremlin Media Spread Coronavirus Disinformation", *RFE/RL*, 18 March 2020; "EEAS special report update: short assessment of narratives and disinformation around the COVID-19/Coronavirus Pandemic (Updated 2-22 April)", EUvsDiSiNFO, 24 April 2020; "Russian intelligence agencies push disinformation on pandemic", *The New York Times*, 28 July 2020.

Information: the emerging operational domain

Historically, technology and science have driven the evolution of violent conflict and warfare across operational domains – from the physical domains of land, sea, air and space, into the more recent and man-made domain of cyber. State and non-state actors have sought to weaponize any new emerging knowledge and discovery to gain an edge over their competitors. This first-mover advantage is particularly powerful during a transition period, until the target has a full appreciation of the conflict instruments at play and is able to design effective countermeasures.

The Alliance is arguably experiencing such a transition period. This analysis posits that NATO became the target of a modern type of warfare, conducted via a new man-made operational domain – the informational one. I view the information operational domain as a virtual global communication environment that allows for information and other links among regular citizens, influence groups and ruling elites. These modern features can unleash unprecedented potential in affecting the political perceptions of its target groups, changing their political preferences, and ultimately, their behaviour. Never in human history has a country (nor as a matter of fact, a non-state actor) had the ability to directly communicate, target and influence the whole population of any other country. An aggressor can use false or manipulated information to alter people's and elites' perceptions, resulting in changes in their preferences, which will then influence politics and policies in the target countries. Interstate aggression is the attempt by one state to undermine or destroy the sovereignty of another state. Therefore, information emerges as a strategic theatre in and of itself, in which NATO's challengers will try to influence the decisions and actions of Allied governments. Examples include Russia targeting African-American voters in the 2016 US presidential elections,[6] or its attempts to influence the results of the UK's EU referendum.[7] Unlike the physical operational domains or even cyber space, the informational domain is not segmented by national borders. The informational domain is therefore unbound by any kind of law or accountability, enabling perpetrators to completely deny any responsibility for interstate aggression.

NATO became the target of a modern type of warfare, conducted via a new man-made operational domain – the informational one

Similarly, the immediate goal of interstate aggression in the information domain is not to facilitate the invasion or coercion of any NATO member state. Instead, the purpose is to weaken and/or destroy – from within – the Organization as a military and political alliance. Its ultimate goal, however, even if pursued indirectly, is similar to that of a classical conventional war: to curtail the sovereignty of NATO countries.

The coronavirus pandemic operates as a powerful enabler. It has been exploited to significantly increase the effectiveness and efficiency of this type of attacks against NATO, using the information domain. The pandemic-related influence operations do not specifically aim to confuse, sow distrust, or deceive and mislead people. These are the means. Instead, the ends are to erode the trust between citizens and incumbent governments: target Allies' internal and social cohesion at the national level; undermine and weaken the relations among Allies at the interstate level; corrode or break the transatlantic link between Europe and the United States.

The Alliance's weak spots

To build an optimal response, NATO would first have to better understand the nature of the threat it is confronting. It can achieve this by deciphering how factors triggering the risks of tearing away or terminating the Alliance are being operationalized by NATO's competitors.

Existing research suggests that there are a few major mechanisms that contribute to the durability (or termination) of a military alliance. One of them is the classical *capabilities aggregation*, meaning that when faced with security threats, states pool military resources to increase chances of defeating their opponent. It is accepted that states generally have two "pure" strategies when faced with a major military threat – to arm themselves or to ally. They can also pursue a variable mix of these strategies. The smaller and weaker countries are less capable of arming themselves independently, which is costly, making it more attractive to join alliances for their defence. The higher the perceived threat is, the more likely that affected states are going to accept the binding arrangements of an alliance. As soon as the threat passes, such alliances have a strong incentive to disband.[8] It is, arguably, this view that directed so many calls for NATO to be dissolved after the collapse of the USSR.

Another dominant mechanism is the *security-autonomy trade-off* model. It posits that in an alliance, some members receive security protection at the cost of a degree of their political autonomy. Other members cover the costs of security, in exchange for an increase in their

6 "Russia 2016 influence operations targeted African-Americans on social media", *The New York Times*, 17 December 2018.

7 UK parliamentary report on Russia, Intelligence and Security Committee, London, 21 July 2020.

8 J.D. Morrow, "Alliances and asymmetry: an alternative to the capability aggregation model of alliances", *American Journal of Political Science*, Vol.35, No.4, Nov. 1991, p.907.

political autonomy.[9] As the security threat diminishes, the militarily weaker allies are incentivised to reduce the amount of autonomy they sacrifice in exchange for security. This may materialize in their reticence to support the policies of the allies who cover the costs of security. For example, France and Germany refused to support the 2003 US invasion of Iraq. This can inevitably create tensions among allies, especially if they do not perceive a major security threat emerging on the long-term horizon.

In democratic countries though – and this is relevant to NATO – the security-autonomy trade-off is strongly impacted by an additional mechanism: *domestic politics*. The logic of this instrument is that state leaders have to consider the opinion of their domestic audience – which is the general public and various influence groups – when deciding on how to invest resources in alliance formation and maintenance.[10] Given the general scarcity of resources and the propensity for building welfare states among European NATO member states, justifying defence expenses while lacking a popular-credible and stringent threat becomes more difficult in genuine electoral democracies. When the information space is exploited as a new operational domain of interstate war, domestic politics becomes extremely vulnerable and malleable to targeted foreign influence operations, due to its globalized and borderless character. As the coronavirus crisis vividly revealed, the interstate confrontation, including attacks against NATO, have shifted from the physical operational domains into the informational one, by targeting populations' perceptions, trust, and support of governmental policies.

Empirical evidence on these mechanisms suggests the powerful impact of the security-autonomy trade-offs and role of domestic politics on alliance duration. In fact, the role and impact of domestic politics on alliance duration in democracies is even more powerful than security concerns.[11] Therefore, anyone interested in maintaining a strong NATO should account for these two factors, especially since the opponents of a strong NATO have grasped their very importance. They are deliberately exploiting and targeting them.

What could destroy NATO?

Recent data suggests a startling trend of dwindling popular support for NATO[12] in a number of its member states. In influential countries such as Germany and France support has dropped, since 2009, to 57 percent (-16) and 49 percent (-22) respectively. The published data for 16 out of 30 NATO countries reveals that support has fallen below 50 percent even in the newer member states such as Bulgaria and Hungary – the figures are 42 percent and 48 percent, respectively. Since 2007, support for NATO dropped to 54 percent (-6) in the Czech Republic and to 51 percent (-2) in Slovakia.

The United States shows now decreasing popular support for NATO at the borderline of 52 percent, which is critically dangerous in times of populism and massive disinformation operations targeting NATO. A referendum to withdraw from NATO, *à la Brexit*, should not be excluded in those countries where support is waning. Hypothetically, this could be achieved through external influence operations exploiting populist agendas, which could bring into power governments that would then initiate referenda on withdrawal from NATO, conducted during times of mass confusion and individual insecurity.

A referendum to withdraw from NATO, à la Brexit, should not be excluded in those countries where support is waning

In addition to aggressively exploiting the domestic factor to undermine the Alliance, NATO's opponents are targeting important elements of the autonomy-security mechanism. Russia, for instance, has long perceived the US as the driving force behind NATO, covering most of the Alliance's security-provision costs. Russian leadership has therefore manoeuvred to weaken the transatlantic link, by decoupling the US from European Allies. Russia did so even when it was the weakest in its modern history.

For instance, on 19 November 1999, during his meeting with US President Bill Clinton in Istanbul, Russia's President Boris Yeltsin privately floated the idea that there is no need for the US to provide nuclear protection to Europe, as Russia could do so as well. Russia's President stated, "Bill […] I ask you one thing. Just give Europe to Russia. The US is not in Europe. Europe should be the business of Europeans. Russia is half European and half Asian". In response, Clinton asked if Yeltsin wanted Asia too. After Yeltsin confirmed that "eventually we will have to agree on all of this", Clinton replied, "I don't think Europeans would like this very much". Yeltsin agreed that not all Europeans would accept it, but then went on to say that "you [US] can take all the other states and provide security to them. I will take Europe and provide them security. Well, not I. Russia will. […] We have the power in Russia to protect all of Europe, including those of missiles […] Russia has the power and intellect to know what to do with Europe".[13]

9 *Ibid*, pp.907-911. Morrow defines autonomy as "freedom to pursue desired changes in the status quo".

10 D. S. Bennett, "Testing alternatives models of Alliance duration, 1816-1984", *American Journal of Political Science*, Vol.41, No.3, Jul.1997, p.850.

11 *Ibid*, p.875.

12 "NATO seen favorably across member states", Pew Research Center, Washington, DC, 9 February 2020. A more fine-grained analysis reveals how misleading the title is.

13 Clinton Digital Libraries, "Declassified documents concerning Russian President Boris Yeltsin", Case number: 2015-0782-M, pp.562-564, https://clinton.presidentiallibraries.us/items/show/57569

These "decoupling" efforts, homing in on the autonomy-security mechanism, continued after Vladimir Putin became president, and are currently at their apex. However, Russia is not just initiating these attempts on the US side. It also actively tries to weaken the transatlantic connection on the European side, employing a push-pull type of strategy. This should not be taken lightly. Polls suggest that in only five out of the 16 surveyed countries – The Netherlands, US, Canada, UK, and Lithuania – does a majority believe that their country should respect Article 5 obligations.[14] The massive disinformation campaign targeting NATO during the coronavirus crisis is an effective tactic in Russia's dual track approach to weaken the Alliance, as the population is particularly receptive to messages linked to its survival or other security needs.

NATO's challengers do not question the technical ability of the Alliance to defend the interests of its Member States. They question NATO's resolve to do it

Sailing into the storm

Providing better security and defence for the citizens of the North Atlantic Treaty Organization requires the ability to understand what the future security threats and risks are, including what could trigger the next interstate aggression and how it is likely to be fought. The state-of-the-art threat assessment today is to look at a host of geopolitical, economic, environmental, legal, informational, and military factors.[15] However, it becomes increasingly obvious that this intellectual framework may not be sufficient to identify and to defeat all foreign aggression attempts against Allies' security. NATO needs to combine its factor-based security assessments with a clear understanding of the relevant conflict mechanisms.

To start, there is a need to re-evaluate what security means in the modern world and to understand the *de facto* emergence of the information space as a new operational domain of interstate war. The pandemic provided a context and testing ground for validating tools and techniques for the effective manipulation and control of a target country's significant segment of the population. It did so by exploiting basic human needs – safety and physical security – and unrestricted information access to the whole target population. This opens interstate aggression opportunities that were previously theoretical and largely hypothetical: breakthrough the enemy's resistance without combat and let the target state's population undermine the government's effective defence and security, including sabotaging NATO's efforts or a vote to withdraw from the Alliance. The main battlespace in the modern conflict *against democracies* is in the information domain; the objective is to target the thinking of the broader public and the subsequent decisions of the governing elites.

What does this mean for NATO? This means, *inter alia*, not only switching NATO's main audience – moving away from its competitors and towards its members' domestic constituencies and influence groups – but it also means extending and improving its toolkit for responding to such new security threats. Specifically, it makes sense to designate the information space as a new operational domain of warfare or interstate aggression, similar to what NATO did with cyber space in 2016. This should allow the Alliance to design and implement planning, doctrine, resourcing and operations related specifically to the information domain. Without this, NATO will be unable to successfully compete in the information space. To the contrary, it is likely to be dominated by challengers like Russia or China, who are benefiting from the first-mover advantage, developing and employing new approaches and strategies on interstate aggression.

Many more measures are to be taken. Some are urgent, and others focus on a longer time horizon. What is critically important is that the current institutional thinking on modern conflict is reviewed. The Secretary General's NATO 2030 initiative appears to provide the suitable context and format for conducting such reflections and refinements.

14 Pew Research Center, 9 February 2020.

15 "Peering into the crystal ball: holistically assessing the future of Warfare", Research Brief RB-10073-AF, RAND Corporation, 2020.

Research Division
Thierry Tardy, PhD, Series Editor
@thierrytardy
NATO Defense College
Via Giorgio Pelosi 1, 00143 Rome – Italy
www.ndc.nato.int

Follow us on Twitter and Facebook
at *https://twitter.com/NDC_Research*
at *https://facebook.com/NDC_Research*
NDC Policy Brief
ISSN 2617-6009