2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

For a Baltic Cyberspace Alliance?

Martin Libicki [1]
Visiting Professor, Cyber Science Department
United States Naval Academy
Annapolis, MD
libicki@usna.edu

Abstract: In NATO, an attack on one is an attack on all. In recent years, this tenet has been extended to mean that a cyberattack on one is a cyberattack on all. But does what makes sense in the physical world also make sense if extended into cyberspace? And if there is virtue in collective cyberspace defense, is NATO necessarily the right grouping – in a world where, as far as the United States and the United Kingdom are concerned, more of what constitutes cyber defense circulates within the Five Eyes coalition rather than within NATO? To explore these issues, this essay moots the creation of a Baltic-area cyberspace alliance, considers what it would do, assesses its costs and benefits for its members, and concludes by considering whether such an alliance would be also be in the interest of the U.S. Keys to this discussion are (1) the distinction between what constitutes an "attack" in a medium where occupation may result and actions in media where occupation is (currently) meaningless and effects almost always reversible, (2) what collective defense should mean in cyberspace – and where responsibilities may be best discharged within the mix of hardness, pre-emption, and deterrence that constitute defense, (3) the relationship between cyberspace defense and information warfare defense, and (4) the relevance to alliance formation of the fact that while war is dull, dirty, and dangerous, cyber war is none of these three.

Keywords: *cyber defense, alliances, NATO*

1 The opinions expressed in this paper are only those of the author, and do not represent the US Naval Academy, Department of Navy, or Department of Defense.

1. INTRODUCTION

Normally, countries do not benefit if their friends go off and form an alliance without them. But cyberspace may be different. The doctrines and arrangements that work in the physical world cannot be transported into the virtual world without asking whether the assumptions that hold in the physical world also apply to the virtual world. This helps to determine if enough tenets remain valid to justify adopting and adapting such arrangements for a new domain, or instead, starting over.

To this end, we moot an alliance of selected European states whose mission is mutual defense against cyberspace threats: operations that degrade, disrupt, corrupt, or destroy information systems, but might also include – largely because of interest in such things in the region – the use of cyber espionage to directly harm another party's interests: e.g., the DNC hack, or similar subsequent intrusions in France and Germany. Selected states, here, include countries that border the Baltic Sea (except, of course, Russia), perhaps with Norway and the Netherlands thrown in for good measure. In such an alliance, the key country would be Germany, but the inclusion of Sweden and Finland means that it would not be a subset of today's NATO. Throughout, we assume the continued existence of NATO as a traditional defense alliance and the continued working of the intelligence-sharing arrangements among the Five Eyes (the U.S., the UK, Canada, Australia, and New Zealand).

In laying out the case for a Baltic cyberspace alliance – a case that should promote both European and U.S. interests – this essay proceeds in several steps. First, we examine the elements of a cyberspace alliance: what tasks it fulfills and whether an explicit alliance is necessary or even helpful to carry out this or that task. Second, we adduce some benefits (again, from both the European and U.S. perspective) to the formation of such an alliance. Third, we discuss issues created by such an alliance.

2. COLLECTIVE DEFENSE IN CYBERSPACE

Central to NATO is the premise that an attack on one is an attack on all: each member is obliged to treat an attack on another member as if it were an attack on itself. Traditionally, the response to an attack was straightforward: a state of war is acknowledged; participating armies defend sovereign territory, attempt to disarm the other side, and have it sue for terms. In the Cold War, the collective strength of NATO's members was used to maintain a front against Soviet invaders, whilst the United States used the threat of a nuclear response to deter Soviet incursions into Europe (or to limit the depth and duration of such an incursion). Although the purpose of an alliance is trickier in domains where aggressors cannot occupy territory

– notably the seas and the air – broad notions such as strength from combining forces and the direct support that such forces can provide to the ground campaign make it straightforward to extend NATO into those two domains.

Conflict in cyberspace is of a different nature, but the nature depends on whether it is tactical or strategic. Tactical cyber war is what supports a kinetic military campaign; it may be a valuable niche capability, but it is the outcome on the ground that matters. A Baltic cyberspace alliance,[2] not being a kinetic military alliance (especially if it included non-NATO countries), would not play in that contest; only individual countries or NATO, collectively, would. If NATO were involved in a real shooting war, tactical and even strategic cyberspace operations could come under NATO's aegis.

Strategic cyber war,[3] by contrast, stands apart from kinetic conflict and may even take place in its absence.[4] One purpose could be to pressure other countries by imposing costs on them; another, conversely, may be retaliation to enable or reinforce deterrence. As a lesser included case, it may be used to enhance influence operations on countries, political groups, or individuals.

It is strategic cyber war for which a Baltic cyberspace alliance might prove useful.

3. NATO AS A CYBERSPACE ALLIANCE

The logic of international alliance is that bigger is usually better when defending against threats.[5] Although the size of the alliance and the need for consensus can complicate warfighting,[6] the concept of a common defense means that an adversary faces the combined militaries of multiple countries. In a world in which attackers are dissuaded by the prospect that united countries will interpose their forces between attackers and those being defended, the premise that more is better makes intuitive sense.

2 The Council of Baltic Sea States, formed after the Soviet Union dissolved, is an intergovernmental organization that works on social, economic, legal, and environmental issues. More recently, Baltic states came together to address currency issues; see "Northern member states unite on euro-zone reform," December 8, 2018; https://www.economist.com/europe/2018/12/08/northern-member-states-unite-on-euro-zone-reform.

3 As defined and used by the author in his *Cyberdeterrence and Cyberwar*, Santa Monica, CA (RAND), 2009 p. 117 -138. See also Tomas Rid, "Cyberwar Will Not Take Place," *Journal of Strategic Studies, 35:1* (2012), pp. 5-32.,

4 Although a cyberattack *can* cause physical damage, it can be considered one more way that cyberattacks can impose costs on societies without necessarily being part of an armed conflict.

5 "Usually" because adding members means getting drawn into more disputes, often in countries that are farther from the alliance's core and therefore harder to physically defend.

6 Good examples can be drawn from the difficulties encountered in Operation Allied Force – in which NATO, incidentally, prevailed; see General Wesley Clark, *Waging Modern War: Bosnia, Kosovo, and the Future of Combat*, New York NY (Public Affairs), 2001.

But combat in cyberspace does not really benefit from economies of scale. Within a country, adding more offensive cyber warriors often means lowering the qualifications (at least initially, and perhaps in the long term) for what is, by nature, an inherently elite profession. This means not only that diminishing returns set in, but that the activities of the good-but-not-great can well tip off the other side. So tipped, the other side can improve its defenses in ways that are specific (e.g., vulnerabilities are patched after having been discovered) and general (i.e., a shift occurs in the tradeoff between security and cost/convenience). Correspondingly, the contribution of additional operators is limited. When these operators come from other countries, their contribution is further vitiated unless these countries operate seamlessly. Within an intelligence-sharing alliance (e.g., the Five Eyes), additional members do add heft (each country, for instance, can employ relationships that it has developed with communications companies around the world). Once seams intrude – and these seams are larger within NATO than within the Five Eyes – the level of coordination is less and the prospects for interference (e.g., two countries seeking access to the same target system) are greater.

When it comes to defense, the arguments that vitiate the benefits mass are different but similar. A large percentage of all cyber defense efforts requires looking after specific systems. Adding allies adds more systems to defend. This hardly helps defenders of existing systems.[7] Although there are defense activities where adding countries may help – e.g., intelligence fusion, collective learning, and forensics – none of these really requires a military alliance, and some of the contributors for these three efforts live in the private realm.

Alliances also express their weight through deterrence policies. In the Cold War, the United States deterred attacks by the Soviet Union on NATO allies with a nuclear threat: certainly, if the attacks involved nuclear weapons, and quite possibly if the attack involved overwhelming conventional force. In recent years the U.S. deterrence policy in cyberspace has been notionally extended to a NATO deterrence policy. Unfortunately, U.S. deterrence policy for attacks on the homeland is already an uncertain thing – and extending it adds further uncertainties. There are, for instance, serious questions about what constitutes a cyberattack serious enough to merit retaliation and what the form of retaliation would be; the United States has used sanctions in response to malign cyberspace activities, but there is little evidence that sanctions have deterred Russia, Iran, or North Korea.[8] NATO's retaliation capabilities – which are largely US retaliation capabilities (plus some UK capabilities) – are even less likely to be brought into play if the target of a cyberattack were European. In the

7 A counter-argument is that larger alliances give foes more targets, forcing them to spread their efforts and thereby relieving defenders of existing systems. But that assumes that (1) all defense efforts counter those foes against whom the alliance is established, and (2) that new allies were not already under attack from such foes.

8 In 2015, China agreed to cease its commercially-oriented cyber espionage under the *threat* of sanctions, but that was more like coercive diplomacy. The agreement unraveled by early 2017 as China perceived that it would be sanctioned over broader trade issues – and so it might as well spy.

five years prior to North Korea's hack of Sony – which the United States did respond to – South Korea suffered far worse depredations with no U.S. response.[9]

4. AND WHY IS THE NATO GROUPING NOT THE OBVIOUS ONE?

Yet Europeans lean on NATO; in large part, because it already exists and therefore does not need to be invented. But NATO is a military alliance, while cyberspace is essentially a conduit for information,[10] hence generally dominated by the community that deals with information *qua* intelligence. And the existence of the Five Eyes coalition only underlines this point: working relationships among that coalition in the information domain are tighter than they are in the information domain across the NATO alliance. And two of the Five Eyes are not even in NATO. In other words, the real coalition is not doing Europe (the UK excepted) in particular that much good. This matters, because the primary cyber war threat to Europe is from Russia, and the primary targets of Russian coercion are in European countries that face Russia. Two of the countries that face the gravest threats are not even in NATO.

Correspondingly, a Baltic cyberspace alliance would have a limited ambit: members would cooperate on defense and aver that a cyberattack on one is an attack on all. In practice, were such an arrangement made, the alliance would have its own definition of what constitutes an "attack"; it might include social media manipulation.

A cyberspace alliance, as such, would have three facets but lack one. The first facet is defense: each country would putatively participate more vigorously in those cyber defense activities that benefit from scale, as noted: threat intelligence, forensics, lessons learned. With very large cyberattacks, they could offer mutual aid for systems restoration. The second facet is defense by deterrence. It would require a consensus on what constitutes an actionable offense in cyberspace, notably the type and severity; what responses are appropriate (e.g., to an attack on the local power grid); and what kind of capability is required to retaliate in cyberspace. One rationale for responding in cyberspace is that less forceful options, such as alliance-wide sanctions, are likely to be even weaker than U.S. sanctions are. Conversely, threatening kinetic responses – given the lack of nuclear weapons among proposed alliance members – lacks credibility thanks to Russia's escalation dominance. The third facet would consist of offensive cyberspace operations used for coercive or, more likely, counter-coercive purposes or

9 Iain Thomson, "South Korea faces $1bn bill after hackers raid national ID database," The Register, October 14, 2014, http://www.theregister.co.uk/2014/10/14/south_korea_national_identity_system_hacked/.

10 Notwithstanding that some of this information (e.g., rogue machine instructions) may result in physical damage.

for retaliation against grave non-cyber offenses (e.g., the Skripal poisonings[11]). By contrast, cyberspace operations in support of kinetic operations (e.g., taking a SAM site offline while a NATO sortie flies overhead) would fall outside such an alliance because kinetic operations fall to NATO; if individual members carried out tactical cyberattacks, they would fall under NATO auspices (or their own fights).

5. CHARACTERISTICS AND ADVANTAGES OF A BALTIC CYBERSPACE ALLIANCE

What are the characteristics and advantages of such an alliance to its member countries?

First, the alliance, limited to cyberspace, would invariably focus on Russia, despite having to tend to other threats (e.g., from China's commercially-motivated cyberespionage) and despite the possibility that alliance members would probably be diplomatic in public about the alliance's purpose. Russia's cyberspace threats are malevolent, politically-directed, and often part of a larger campaign to sow disorder and facilitate coercion. NATO countries, as a whole, are not entirely focused on Russia, these days: those in North America pay as much attention to China;[12] those near the Mediterranean tend to look southward.

Second, such an alliance would include currently neutral countries, notably Sweden and Finland. Both countries punch above their weight, in cyberspace operations[13] and information operations[14] respectively. This raises the question: why don't such countries just enter NATO? To be sure, roughly half the citizens in both countries would like to – but the other half fear, justifiably, a neuralgic Russian reaction if they did (Finland's accession could put troops along miles of Russian borders). Although Russians would likely react badly to the formation of a Baltic cyberspace alliance, they would have a more difficult time summoning images of jackbooted soldiers while doing so. For Sweden and Finland, the cyberspace alliance could serve as a halfway house. If the Russian threat eases, their entry into NATO can be indefinitely postponed (in the unlikely event that the Russian cyberspace threat disappears, they can leave or the cyberspace alliance might wither away). If the Russian threat persists

11 See, for instance, Larisa Brown, "Theresa May could order a cyber attack against Russia in retaliation for the nerve-agent strike as part of a secret package of measures to hurt Putin," March 12, 2018; http://www.dailymail.co.uk/news/article-5492835/Theresa-order-cyberattack-against-Russia.html.

12 Just one small sample: Ryan Browne, "New acting secretary of defense tells Pentagon 'to remember China, China, China'," January 2, 2019;https://www.cnn.com/2019/01/02/politics/shanahan-pentagon-first-day-china/index.html.

13 See, for instance, Hugh Eakin, "The Swedish Kings of Cyberwar," https://www.nybooks.com/articles/2017/01/19/the-swedish-kings-of-cyberwar/, January 13, 2017.

14 See, for instance, Reid Standish, "Why Is Finland Able to Fend Off Putin's Information War? Helsinki has emerged as a resilient front against Kremlin spin. But can its successes be translated to the rest of Europe?" March 1, 2017; https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/.

or worsens, these two countries will have had more practice interoperating with NATO countries, thereby easing their way into an alliance that spans the conventional domains of warfare.

Third, a cyberspace alliance would be a mechanism to get Germany to become more involved – or, more to the point, take leadership – in defending Europe against Russia. The current contribution of German military spending (1.2 percent of GDP) to the common defense of NATO is modest. Germany, nevertheless, remains Europe's largest economy, and would constitute roughly half of the weight of any Baltic cyberspace alliance. Germany has also stepped up smartly in developing its Cyber and Information Domain Service. Its manning, if plans hold,[15] would constitute 7.5 percent of Germany's total force level (13,500 out of 180,000);[16] its spending would be 6.3 percent of Germany's military (41.5 billion Euro) budget.[17] By way of contrast, USCYBERCOM's end-strength goal of 6,000 compares to 1.3 million military personnel in the overall U.S. military – less than a tenth as much concentration on cyberspace. Granted, this is not an apples-to-apples comparison: Germany's end-strength includes electronic warfare battalions; USCYBERCOM's end-strength does not. But, even after adjustments, Germany's commitment to fighting in cyberspace, relative to its overall military strength, looks more substantial than the U.S. commitment. Furthermore, a German focus on cyberspace (vis-à-vis kinetic elements of military power) is, again, less likely to engender a neuralgic reaction from Russia (no jackboots, etc.) but does put Russia on notice that its maneuvers in cyberspace have not gone unnoticed and will be resisted by those best placed to resist them.

The advantage of such an alliance to its members is that they put the power of all in service of each. This should give Russians second thoughts about their use of cyberspace for offensive purposes – although it may also initially goad them into carrying out operations against the non-NATO countries (Sweden and Finland) to inhibit their participation in such an alliance. Russia's doing so, conversely, could very well reinforce the value to today's neutral countries of having others to lean on when facing Russia. The countries in this alliance would be self-selected by virtue of their concern over Russian activities in cyberspace. By contrast, a unified and meaningful NATO response to Russian provocations has to surmount the objections of countries that reserve some sympathy for Russia (Hungary and Greece come to mind).

15 "Defence Minister Ursula von der Leyen revealed plans to recruit up to 13,500 cyber soldiers in addition to around 500 civilian workers capable of defending the military's electronic intelligence as part of the new Cyber and Information Space Command, according to Germany's *The Local*." From Tom O'Connor, "German Military Battles Foreign Hacking with New Cyber Soldiers," April 5, 2017; https://www.newsweek.com/german-military-launches-new-cyber-division-amid-russian-hacking-claims-579573. In the interim, many of its employees could be reservists, though; "Germany struggles to step up cyberdefense," August 7, 2018; https://www.dw.com/en/germany-struggles-to-step-up-cyberdefense/a-44979677.

16 The UK's formation of a 2,000-person strong *cyber* force, within an armed force of 160,000 total members, also suggests a higher percentage commitment to cyberspace than in the United States; see David Bond, "Britain Preparing to Launch New Cyber Warfare Unit," Sep 21, 2018, https://www.ft.com/content/eef717f2-bb6e-11e8-8274-55b72926558f.

17 Sumi Somaskanda, "Cyberattacks Are 'Ticking Time Bombs' for Germany," June 4, 2018; https://www.theatlantic.com/international/archive/2018/06/germany-cyberattacks/561914/.

Fourth, this would give NATO competition in the alliance business. Arguably, this would weaken NATO – and is thereby a disadvantage. But competition can also be good: it persuades competitors to listen to their clients (customers, audience, etc.) and induces them to innovate in order to retain their standing. Otherwise, secure in the knowledge that their position is unassailable, they risk becoming sluggish and unresponsive – and when they fall or come apart, it is often "first slowly and then all at once".[18] Thus, when offering cyber security or countering cyberattacks, relevant countries can ask the institutions of NATO and also those of the Baltic cyberspace alliance what each of them can do – each knowing that they are competing both against Russia's malign influence and the other's benign influence. But competition can also raise problems: an institutionally aggressive cyberspace alliance may seek greater influence by stretching the definition of a cyberattack: e.g., to include electronic warfare, interference with space operations, and sabotage of or attacks on information infrastructures.

6. ADVANTAGES FOR THE UNITED STATES

The most basic advantage is that it makes Europeans more responsible for their own defense, albeit in just this one domain. In the 1980s, for example, three neutral countries – Switzerland, Sweden, and Finland – spent far higher proportions of their income on national defense than most European NATO allies did.[19] The "free rider" problem is, if anything, worse today. It may be that much more difficult to persuade European countries to arm themselves if, when such arms have to be used, it would be under a war effort led by the United States. The return of Russia as an aggressive power, since roughly late 2013, may not have been internalized by European countries, concerned as they are with internal fissures – many of which, ironically, were deliberately exacerbated by Russia's information warfare campaign. And the U.S. pivot to Asia, while more advertised than practiced, would necessarily mean a shift in U.S. resources that would otherwise be available for Europe.

But in cyberspace, countries in a Baltic cyberspace alliance would be pooling their resources under either their own individual command (as befits an activity so highly linked to intelligence) or, at least under the command of Europeans. And with the United States not in such an alliance, there is much less of a "free rider" problem (even if Germany would be roughly half the alliance, countries such as Sweden, Finland, and Estonia punch above their weight in this domain). The downside of the upside is akin to the owner of a hammer being persuaded that every problem is a nail: if given a choice between responding to hostile actions in the kinetic world and responding in cyberspace, the latter may be seen as particularly attractive because it

18 The quote is from Ernest Hemingway's *The Sun Also Rises*.

19 Each of the two NATO countries that *did* invest heavily in national defense – Greece and Turkey – largely did so to keep the other at bay.

relies on tools the alliance can wield themselves rather than tools largely wielded by the United States.

Another advantage for the United States is that such an alliance may complicate Russia's cyber war efforts – largely by increasing the uncertainty that Russian efforts may be met with reprisals: the odds of retaliation from either the United States (as the premier cyberspace power of NATO) or from the Baltic cyberspace alliance will be higher than the odds of retaliation from each of them. This is particularly true for those cyberattacks that leave multiple victims: NotPetya, as an example, levied costs in the hundreds of millions of dollars from Merck and Federal Express (both U.S.-headquartered corporations) and from Maersk (headquartered in Denmark). The raised odds for a response may arise from meeting credibility thresholds (the United States may be wary and the Baltic cyberspace alliance less so or vice versa), attribution thresholds (the United States may have confidence and the Baltic cyberspace alliance may not or vice versa), and damage thresholds (the United States may recognize a higher threshold to warrant its retaliation if the effects of the cyberattack fall primarily on Europeans). Both the United States and the Baltic cyberspace alliance may retaliate but against different targets.[20]

An associated benefit is that if the *modus operandi* of whatever cyberspace operations ensue from NATO (that is, in practice, from the United States or the UK) and the Baltic cyberspace alliance are sufficiently similar, it may not be clear to Russia who struck back. This would complicate counter-retaliation targeting (and threats), in anticipation of which retaliation may be more likely, and the prospect thereof more credible. To be fair, attack-retaliation cycles in cyberspace remain loose: the closest example of a retaliatory cyberattack was the late 2012 DDOS campaign against U.S. banks by an Iran that had, two years earlier, discovered that its nuclear program had been set back by the Stuxnet worm. Attack-retaliation-counter-retaliation cycles are even more n^{th}-order relationships. Furthermore, Russia may have the SIGINT or HUMINT to make its own attribution – or it may not care and may conclude that the Baltic cyberspace alliance is an arm of NATO despite the former having neutral countries in it; indeed, it may see all opposing alliances as arms of the United States, facts notwithstanding.

Second-order considerations add complexities:

- Conceivably, neither NATO nor the Baltic cyberspace alliance retaliates in the belief that the other will – and that letting the other one do so may avoid counter-retaliation while gaining the benefit of deterrence (to wit, the "free rider" problem that affects NATO, writ large). Perhaps each side may interact with the other, but because cyberspace operations are so highly classified,

20 Perhaps needless to add, if the United States has high confidence in attribution and high thresholds, and the Baltic cyberspace alliance has low confidence in attribution and low thresholds, neither may decide to retaliate.

each side may conclude that the failure to hear from their counterpart is no evidence that nothing is being planned – and so each assumes that the other is making plans.

- There could well be an exchange of intelligence between NATO and the Baltic cyberspace alliance that allows attribution evidence on Russian cyberattacks to strengthen the case over what each may conclude from its own efforts. That raises the question of why countries – the owners of intelligence services – do not simply cooperate within NATO to build that case. First, Sweden and Finland are not NATO members (although, as noted, Sweden shares information with the West). Second, a Baltic cyberspace alliance may well induce member countries to raise their cyber intelligence game (because they are helping themselves rather than others) giving them more to contribute.
- Just as having two independent sources of threats complicates Russia's calculus, it can also complicate the assurance component, wherein others are assured that small attacks will be treated less harshly than large attacks lest others lose any reason to moderate their bad behavior (colloquially: "in for a dime, in for a dollar"). An early version of this logic explains why Robert McNamara (the 1960s-era U.S. Secretary of Defense) was unhappy with France's nuclear capabilities and ambitions. If nuclear war ensued, he wanted the option of using nuclear weapons first against the nuclear systems of the USSR but not targeting cities specifically – and then threatening that if the USSR did strike Western cities, the United States, in turn, would target Soviet cities. But France's nuclear deterrent was too small to be used against Soviet nuclear installations exclusively – it was meant solely as a deterrent. Thus, if France used its nuclear weapons against Soviet cities, there would be little reason for the USSR to avoid hitting U.S. cities – even if the United States did not initially target Soviet cities. Again, the imprecision, loose coupling, and ambiguity associated with cyberspace operations may make this consideration notional for the time being.

7. THE RISKS OF ENTANGLEMENT

A classic problem of the politics of an alliance is the scope that it gives members, particularly the smaller ones, to get partners wrapped up in their fights. Take WWI: what was initially an Austrian-Serbian fight became a Russian-Austrian-Serbian fight, and then a German-Russian-Austrian-Serbian fight before morphing into a Franco-German-Russian-Austrian-Serbian fight. With two alliances, one specific to a particular domain, the complexities quickly mount (even ignoring a highly unlikely

cyberattack by a NATO member outside the Baltic cyberspace alliance on a non-NATO member inside the alliance).

One entangled path may arise from a retaliatory cyberattack by a member of the Baltic cyberspace alliance which yields a kinetic retaliation. If this kinetic retaliation is considered an attack, and if the target state is a member of NATO, then an Article V issue arises; if NATO members agree, what was started by a non-member of NATO in cyberspace could descend into a kinetic conflict between NATO and Russia. Granted, NATO does not have to respond; it may argue that it played no role in the initial fracas – but a failure to invoke Article V under circumstances that would call for doing so would harm NATO's credibility as an alliance.

Another path is the conflation of information warfare with its subset,[21] cyber warfare – coupled with the latter's conflation with kinetic war. Somewhere on the spectrum between mischievous speech and Armageddon, every alliance needs to draw some line between acceptable and unacceptable practice. Otherwise, a country's (admittedly malign) attempts to manipulate social media messaging will start other countries down a slippery slope. Of this, several observations. First, a hard line on freedom of speech (and press) is baked into the U.S. Constitution. Europe is more apt to weigh such freedoms against community values (e.g., prohibiting hate speech and enhancing privacy and data protection). When mobilizing to "counterattack" unwanted expression, a U.S.-dominated NATO may be more reluctant than a Baltic cyberspace alliance (although the greater U.S. bent towards action could balance this out). Second, all this potential conflation suggests the need for any such alliance posture to make distinctions among levels of conflict – separating influence operations from cyberattack; cyberattack from kinetic attack; and conventional kinetic attack from nuclear attack. To proclaim that "an attack on one is an attack on all" without defining "attack" draws no such distinctions. Such levels may have to be crossed – the hypothetical cyberattack that kills thousands may outrank an exchange of naval gunfire at sea, for instance – but crossing should be a deliberate act; one, moreover, that reflects alliance consensus. There also needs to be room for some intra-war deterrence so that Russia does not heedlessly escalate from one level of hostility to another.

A third path leads from intelligence to operations. The two influence one another in all media, but the relationship is particularly close in cyberspace – where a penetration made for one purpose can be used for another and where a successful and persistent penetration is often the major part of any such operation. Problems may arise because friends spy on one another. In one infamous example, the NSA reportedly tapped the private phone used by Germany's Chancellor.[22] Although systems that are targets for cyber espionage are often implausible places to start a cyberattack from, exceptions

21 As the author argues in "The Convergence of Information Warfare," *Strategic Studies Quarterly*, Spring 2017, 49-65.

22 Melissa Eddy, "File Is Said to Confirm N.S.A. Spied on Merkel," July 1, 2015; https://www.nytimes.com/2015/07/02/world/europe/file-is-said-to-confirm-nsa-spied-on-merkel.html.

exist – and when malware is found, the target may be persuaded to overlook such distinctions to draw implausible conclusions. A Baltic cyberspace alliance may provide a mechanism for countries to develop a consensus on how aggressive cyber espionage could become without triggering Russia to retaliate out of fear of a pending cyberattack.

A fourth path arises from trying to distinguish between tactical cyberattacks carried out to support kinetic operations, and thus under NATO auspices, and strategic cyberattacks that could come under the auspices of a Baltic cyberspace alliance. Presumably, because the usefulness of tactical cyberattacks in the absence of kinetic conflict is minimal (because disruption, unlike destruction, can be reversed in short order), if there is no kinetic conflict at hand or on the horizon, there is no tactical cyberattack – everything else therefore is of a strategic nature and hence could come under the aegis of the Baltic cyberspace alliance. But the tactical-strategic divide is not at all a canonical one and, even if it were, there are tricky edge cases: e.g., implants into weapons systems at times of peace, cyberattacks against dual-use infrastructures (especially those European-wide), weaponized cyberespionage against European national security establishments and their members, and a heavier electronic jamming environment.

Finally, whatever alliance efforts (over and above national or private efforts) are made to secure dual-use critical infrastructures, they would have to be deconflicted so that NATO and the Baltic cyberspace alliance do not trip over each other being helpful. This is mostly a notional concern given the limited contribution that any outsider group (much less a foreign outside group) can make to defending specific networks.

8. ROADS NOT TAKEN

Among the objections to a Baltic cyberspace alliance is that there are other European institutions to take care of the matter, and that the countries best suited for such membership may not necessarily be Baltic at all.

One such institution is the EU. Because cyberattacks can influence economic and political well-being, there is a natural compatibility between the EU's mission and collective action to help promote cybersecurity. Certain critical infrastructures under threat from cyberattack, notably the electric grid, span the EU. Correspondingly, the EU is a vital participant in whole-of-infrastructure protection efforts. But cyber security is not just a matter of hardening networks and systems. It involves intelligence to understand how and why such systems may be attacked and it may

involve active defenses to stymie imminent and ongoing cyberattacks.[23] There may also be circumstances where reprisals may be called for; even if some reprisals such as economic sanctions can be organized under EU auspices,[24] those that involve cyber operations are, again, incompatible with the EU's purpose. Intelligence, active defenses, and retaliatory cyberattacks are, instead, actions of national security communities.

The question of membership in the Baltic cyberspace alliance involves tradeoff: more members means more clout but also less focus and possibly less consensus. As noted, Norway and the Netherlands may be useful members of such an alliance even though neither abuts the Baltic. What about France? On the one hand, France's emphasis on cyberspace[25] looks much like Germany's, and the bilateral relationship between France and Germany can be understood as the cornerstone of Europe's stability. On the other hand, geography (e.g., distance from Russia) and history (e.g., former colonies) may lead France to different perspectives from Germany on the Russian threat from cyberspace. What about the UK? On the one hand, the UK government's skepticism regarding Russian intentions is well understood, and its GCHQ brings considerable assets to the fight in cyberspace. But the UK is part of the Five Eyes group; thus, any intelligence-sharing arrangement the UK has with Baltic states necessary means similar intelligence-sharing arrangements with all the other Five Eyes members (notably, the United States), who may be uncomfortable with such sharing. Furthermore, the advantage of ambiguity afforded by having two independent alliances taking on Russia in cyberspace would be vitiated if both alliances contained the same member.

9. CONCLUSION

A hypothesized Baltic cyberspace alliance, along the lines laid out above, would send a strong signal from Europe that it intends to oppose Russia's hybrid warfare activities in general and its information warfare campaign in particular. It would add complexities and uncertainties to Russia's aggressive campaigns, and should thereby slow them down and make them easier to counter.

23 Reportedly, U.S. Cybercommand stymied 2018 Congressional election interference by blocking Internet access enjoyed by Russians' Internet Research Agency. Ellen Nakashima, "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," February 26, 2018; https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff3-22e9_story.html.

24 "In joint conclusions after the EU summit, heads of state denounced aggressive cyber action but stopped short of signaling a move toward decisive EU deterrence against Russia." From Laurens Cerulus, "Russia dodges bullet of EU sanctions on cyber -- for now," October 18, 2018; https://www.politico.eu/article/russia-dodges-eu-sanction-on-cyber-for-now/.

25 France plans a cyberspace force of 4,000 by 2025; see Arthur Laudrain, "France's New Offensive Cyber Doctrine," February 26, 2019; https://www.lawfareblog.com/frances-new-offensive-cyber-doctrine.

The most obvious alternative to such an alliance would be to strengthen NATO's cyberspace capabilities – which is already going on.[26] But the paper argues that a Baltic cyberspace alliance that operates above the tactical level (because it would not support kinetic operations) would offer several advantages. It would bring in friendly but neutral countries, allow Germany to exercise a leadership role in European defense, and have the countries in Europe most affected by Russian mischief cooperate in warding it off. Even some of the disadvantages – it might compete with NATO – can be advantages (competition is good). But most of all, it complicates Russian decision-making as regards cyberspace by making threats of retaliation more credible and harder to counter-deter.

26 Not only has NATO declared cyberattacks an Article 5 issue, but in late August 2018, NATO established a military command center able to mount its own cyberattacks with capabilities offered by the United States, Britain, Estonia, and others. From Robin Emmott, "NATO cyber command to be fully operational in 2023," October 16, 2018; https://www.reuters.com/article/us-nato-cyber/nato-cyber-command-to-be-fully-operational-in-2023-idUSKCN1MQ1Z9.