The Chicago Council on Global Affairs

Transatlantic Paper Series No. 3
October 2010

A Common Future? NATO and the Protection of the Commons

Michael Horowitz

The global commons, areas of the world that fall outside national sovereign control including air, sea, space, and cyberspace, is an area of growing concern for the United States and its NATO allies. This paper argues that NATO has a potentially vibrant role to play in helping ensure open and secure access to the global commons. Investments to counter emerging threats, including cyber threats, would fit the defense budget constraints facing many NATO members while simultaneously serving an important strategic purpose. In particular, new NATO cooperation to face cyber challenges from both state and non-state actors can serve a critical role in protecting NATO members from cyber attacks. However, renewed cooperation in the cyber and space commons will require resolving uncertainty about the relationship between a cyber attack and a kinetic attack, and the conditions for a justifiable cyber retaliation.

The future role of NATO is more uncertain now, in the period leading up to the Strategic Concept review in fall 2010, than at any previous point in NATO's history. In the United States, critics of NATO continue to multiply as they view the value of the organization as lessening, and question whether the United States can and should continue to provide security to Europe through NATO as the global financial crisis continues. In Europe, diverging security perceptions have led some on the continent to wonder what *they* are getting out of NATO, other than blowback in the form of terrorist incidents from U.S. adventures abroad. While this clash of values plays out on a daily basis in NATO's deployment in Afghanistan, looming on the horizon is the question of its role in the global commons.

The global commons, areas of the world that fall outside national sovereign control, is an area of growing concern for the United States. Control of the commons is fundamental for U.S. military operations, as it enables missions ranging from the 1999 air campaign in Kosovo to the ongoing counterinsurgency (COIN) operations in Afghanistan. Yet, the assumption that the United States will maintain superiority in the air, naval, cyber, and space realms is far from a certainty. In fact, concern over the commons has triggered a wave of research on the topic and references to its importance in the latest Quadrennial Defense Review (QDR).[1]

This paper argues that while NATO's critics have raised legitimate concerns about its future, it still has a vibrant role to play in helping ensure open and secure access to the global commons. Collaboration between the United States, Canada, and the European member states of NATO can serve a vital role in bolstering the security of all

The Transatlantic Paper Series is a product of The Chicago Council on Global Affairs' project on "The Future of the Transatlantic Alliance in a Changing Strategic Environment." The project was made possible by generous funding from the Robert Bosch Stiftung, the McCormick Foundation, and the Adenauer Fund at The Chicago Council on Global Affairs.

Michael Horowitz is an assistant professor of political science at the University of Pennsylvania and a senior fellow at the Foreign Policy Research Institute. He has also held fellowships at the Olin Institute for Strategic Studies at Harvard, the Belfer Center for Science and International Affairs at Harvard, and the Weatherhead Center for International Affairs at Harvard. His first book, The Diffusion of Military Power: Causes and Consequences for International Politics *<http://press.princeton.edu/titles/9204.html> was recently published by Princeton University Press.*

NATO members, not only in the traditional areas of air and sea power, but also in the cyber and space realms. While the European member states of NATO are unlikely to invest heavily in recapitalizing their militaries, lower-cost investments that can counter emerging threats, including cyber threats, might better fit their budgets and serve an important strategic purpose. Reinvigorated NATO activities could therefore help NATO members defend against growing cyber challenges from both state and nonstate actors. Renewed cooperation in the cyber and space commons will require allies to address several uncertainties, including the relationship between a cyber attack and a kinetic attack, and the conditions for a justifiable cyber retaliation. On the sea, NATO collaboration will continue in areas such as anti-piracy operations. NATO faces numerous challenges but has a potentially vital role to play with respect to protecting the traditional and new commons.

NATO's End?

NATO is currently undergoing a review process in preparation for a fall 2010 summit designed to create a new Strategic Concept or overarching strategy.[2] The review has revealed that, in some ways, NATO is more active now than ever. Approximately 70,000 NATO-aligned troops are currently deployed across the world in land, air, and naval operations.[3] Ivo Daalder and James Goldgeier state that NATO "has gone global" and that "NATO's expanded ambit is a direct result of the new global politics that emerged after the Cold War."[4]

Significant tensions, however, threaten NATO's fabric as an operational military alliance. At a NATO Strategic Concept seminar in Washington, D.C. on February 23, 2010, U.S. Secretary of Defense Robert Gates stated that NATO is experiencing an internal "crisis."[5] Since the end of the Cold War, NATO has transformed from a primarily defensive alliance designed to protect its members from attack by the Soviet Union to an expeditionary alliance attempting to ensure peace and security abroad. NATO shifted from having one overwhelming and specific reason for its existence to a more nebulous, general purview. One concern Gates raised about this transformation was that many NATO members are not spending enough to ensure their own defense. A multinational, high-level panel on NATO's future chaired by former U.S. Secretary of State Madeleine K. Albright recently concluded that the unwillingness of many European nations to spend enough on defense is hindering NATO's transformation into an effective twenty-first century military alliance.[6] In 2009, of the United States' NATO partners, only Bulgaria, France, Great Britain, Greece, and Turkey spent more than two percent of their gross domestic product on their militaries.[7]

Gates also pointed to a deeper, cultural test that has emerged for NATO. While one of Europe's great achievements was pacifying after centuries of warfare, Gates believes that its unwillingness to consider using military force and spending money on its military risks inviting aggression.[8] A panel of senior advisers convened by the Atlantic Council came to the same conclusion in a report released this year, arguing, "Today too many allies lack a shared conviction of the Alliance's core commitments and their own responsibilities, and without it no alliance (nor indeed Union) can survive over time."[9]

Miscommunications, residual hurt feelings from the Bush administration years, and domestic politics have all hindered cooperation, but genuine shifts in interests may also play a role. If the United States perceives the world as more dangerous than many of its European allies do, these states will unsurprisingly spend less on defense and worry more about the United States provoking threats rather than solving them.[10]

Even when European governments and elites see the threats that the United States sees—or wish at least to support their ally—their publics do not always agree. The Dutch electorate became the only European public to toss a government out of office in part due to its opposition to troop deployments linked to the global war on terrorism.[11] Zaki Laïdi, a professor at the College of Europe, argues that Europe has become extremely risk averse, in part due to the preferences of many European publics.[12] Creating a sounder footing for NATO therefore

requires focusing NATO more on emergent threats that both the United States and its European allies find intrinsically compelling based on their interests and capabilities, rather than assuming that all members want to assist or have the capability to help in all situations.

Emergent Threats to NATO Members

What are the most likely threats facing NATO members and how should the United States and its NATO allies consider using NATO to address them? The fundamental responsibility of NATO remains protecting its members from territorial challenges, especially foreign invasion. As the Albright report notes, this type of scenario is extremely unlikely but "cannot be ignored."[13] The Atlantic Council report on NATO's future similarly recognizes that while territorial defense is the "core" threat NATO is designed to address, it is not the issue NATO member states are most likely to face over the next decade.[14]

Instead, statements about NATO's future role often focus on an array of post–Cold War security concerns, including nuclear proliferation and terrorism. Yet, these are issues where divergent threat perceptions and lagging European conventional military power make it increasingly hard to cooperate effectively. These issues are also reasonably well known, though debate about the optimal way to address them is ongoing.

Defense analysts in the United States increasingly regard discussing the "global commons" as a useful way to think about some of the security challenges that transcend national borders. As defined above, the global commons are those areas that fall outside of the specific sovereignty of any nation-state. Thinking about the security dimension of the global commons is nothing new—for example, there is a rich history of research on the national security dynamics pertaining to the oceans, which Alfred Mahan, among others, studied over the last few centuries.[15] The notion of what exactly constitutes the commons, however, has greatly expanded over the last hundred years and now incorporates air, space, and cyber dimensions.[16] Thinking about the global commons may also help move debates about the future of NATO forward, since its members collectively face a new array of security threats in these realms. Framing dialogue in terms of the global commons is a potentially productive way to outline the possibilities for cooperation between the United States and its allies. It shifts the discussion to focus on those areas where international collaboration is essential.[17]

A large measure of U.S. power, and thus the power of NATO, derives from its command of the global commons. It is in the global commons where international business is conducted and where U.S. naval and air power guarantee the security of the American and NATO homelands from conventional military attack. All NATO states have inherent interests in ensuring safe commerce and open seas and skies. This shared view of the importance of the commons means greater collaboration may be possible in some areas.

Cyberspace in particular is an emerging national security arena that transcends national borders and requires consideration as a new domain of the commons.[18] No nation can accurately claim that it either dominates the domain or has a perfectly successful policy for its regulation. It is also man-made, in contrast with the other, naturally existing areas.[19] While a great deal of civilian activity occurs in cyberspace, a large degree of national security activity also occurs there, making it a natural area for investigation by NATO member states. Concerns about cyberspace security have existed almost from its beginnings. For example, the RAND Corporation has published more than a dozen reports on the national security implications of cyberspace since the 1990s.[20] The 2010 QDR lists operating in cyberspace as one of the six most important tasks facing the U.S. Department of Defense (DOD).[21] The global economy and advanced militaries of the world increasingly depend on cyberspace for their operations. In the economic realm, whether it is to facilitate global e-commerce, ensure safe currency transactions across borders, or monitor the safety of power plants, safe and stable access to the Internet is a necessity rather than a luxury.

Many members have now recognized that cyberwarfare is an important issue for NATO to address. The existing interdependence of some information systems shared by NATO partners mean a massive cyber attack on the United States, or nearly any member of NATO, could have large-scale consequences for other members. For example, a sustained denial of service attack or virus that took down power grids in Germany would have enormous economic consequences for not only Germany but the United States, and other NATO allies as well. Similarly, a successful cyber attack against a computer linked to a NATO network in Brussels could spread to computers in Berlin or even Washington, D.C.[22] Many of the cyber attacks over the last decade that have been severe enough to motivate renewed NATO concerns about cyberspace have emanated from Russia. Given that the security challenges created by the Soviet Union drove the creation of NATO in the first place, these cyber threats arguably represent a core mission area for NATO that returns NATO to its roots. Addressing cyber threats thus arguably fulfills NATO's most basic security mission. Indeed, the most likely scenario for a sustained strategic cyber attack on a NATO member state may involve a Russian cyber assault against a newer member of NATO in Russia's traditional sphere of influence.

As the recent National Academies report on cyber attacks clearly demonstrates, most thinking on cyber security tends to focus exclusively and unsurprisingly on defending western networks,[23] as the DOD is subject to thousands of attempted cyber attacks, from denial of service efforts to hacking, every day.[24] Additionally, cyberspace facilitates real-time communication between soldiers on the ground around the world and the Pentagon, communication between unmanned aerial vehicles (UAVs) and their operators, and dozens of other tasks. Predator strikes in Afghanistan, for example, rely on operators at military bases in the United States to fly the drones. Disruptions to those data linkages would significantly hinder not only UAVs but also most of the International Security Assistance Force (ISAF) operations in Afghanistan. Diverse groups ranging from insurgents in Afghanistan to the Chinese military have written about the dependence of the West in general and the U.S. military specifically on cyberspace, along with potential ideas for disrupting Western and specifically U.S. access.[25]

These writings and ideas are being translated into action. Several incidents over the last several years have revealed the systematic risks from cyber attacks.[26] Prior to the Russian military excursion against Georgia in August 2008, Russia launched weeks of cyber attacks designed to disrupt servers run by the Georgian government, media, and industry. The attacks continued even after the conflict on the ground ceased.[27] In early 2009, Canadian sources revealed the presence of a Chinese-based hacking operation called GhostNet that had infiltrated government computers in 103 countries. Targeted computers ranged from those used by the Dalai Lama to some NATO machines.[28] In April 2007, Estonia suffered a severe denial of service and hacker attack that was traced to Russia. The attack was reportedly linked to Estonian efforts to further distance itself from Russia. While no direct public evidence linked the Russian government to the attack, many Western sources have accused Russia of complicity, if not participation, in the effort.[29] Reportedly, beginning in 2003, hackers based in China participated in an operation labeled by the United States as Titan Rain. The hackers attacked computers at U.S. defense contractors, including Lockheed Martin, as well as U.S. government computers, seeking to steal classified information about U.S. defense programs.[30]

These examples are not exhaustive, but they demonstrate the prevalence of risks to cyber security and the potential national security implications of cyber attacks. Additionally, the traditional framework for assessing control of the commons—as well as threats to NATO—tends to assume that the nation-state is the only actor of relevance. Yet, nonstate actors will have a growing role, especially in the cyber realm. As innovation in the information age relies as much or more on individual creativity than industrial might, so can smaller states or nonstate actors more easily leverage cyberspace over other areas of military power over the next

generation. The United States and its NATO partners have to consider cyber challenges emanating from both nation-states and nonstate actors, including terrorist groups.

Cyberspace is also a realm where traditional notions of deterrence may break down. Deterring a threat by issuing counter-threats to deliver a devastating response to any cyber attack against the United States and its NATO allies may seem like an attractive solution to the cyber security challenge. The high costs associated with defending networks from cyber intrusions and the relatively low costs of launching a cyber attack have led many to analogize cyber deterrence to nuclear deterrence.[31] However, cyber attacks lack the stable footprint of conventional military forces. The fact that terrorist attacks do not leave a "return address" is accentuated in the case of cyber warfare. In the case of a cyber attack, for example, even tracking down the specific computer from which an attack was launched might not give the attacked country sufficient information to distinguish whether a country, terrorist group, or rogue individual launched an attack from that particular computer. These concerns, in part, are why U.S. Deputy Secretary of Defense William Lynn recently stated that denying adversaries access to U.S. information systems in the first place, rather than planning to retaliate in case of an attack, encompasses the bulk of U.S. defensive efforts.[32] The United States and its NATO partners must invest heavily in defending their networks from intrusion and cannot be confident that maintaining nascent retaliatory capabilities will suffice to deter attacks. Furthermore, while strong cyber ties between NATO members might not ensure that deterrence succeeds, weak cyber ties will almost certainly encourage adversaries to launch more cyber incursions against NATO members.[33] Finally, since many future wars will likely include major cyber components, thinking about cyberspace as a very separate sphere of warfare delinked from other areas of conflict is counterproductive.[34]

Outer space is another area where NATO will face emerging challenges. Protecting economic and military assets in space is an increasingly crucial issue for the United States and NATO as a whole. While the United States has the most extensive satellite architecture in NATO, the EU and fourteen other NATO member states also operate satellites.[35] Anyone–even an insurgent—can potentially purchase time on a commercial satellite, affording him access to reasonably sharp imagery and accurate location tracking. Satellite-based location tracking could then help a group plan an attack on a military or civilian asset, or track large troop movements. In the commercial realm, access to space affects everything from predicting weather forecasts to time stamping financial transactions to helping people find their way when they get lost on the road.[36] The United States depends on secure, real-time access to its satellites in space for tasks such as sending data from surveillance drones to troops on the ground below, and precision guiding its weapons. As U.S. dependence on space has increased, so has the vulnerability of its satellites. Chinese analysts studying the future of warfare against potential high-technology adversaries—e.g. the United States—frequently discuss procedures for severing the link between the United States and its space assets.[37] This could occur either through disrupting communications or with anti-satellite weapons, which the Chinese have already tested.[38] The continuing spread of ballistic missiles and missile technology around the world is increasing the number of countries able to launch satellites into orbit—and able to shoot them down. Therefore, finding ways to harden space assets against attack and to ensure redundancy in case of a successful attack is of utmost concern to NATO members. Since ensuring redundancy could require cross-national utilization of satellites during crisis periods, addressing the issue through a preexisting military alliance such as NATO could facilitate easier cooperation than might otherwise occur.

These emerging areas—cyber and space—of the commons may present opportunities for renewed cooperation within NATO. NATO members already collaborate on many issues, including significant naval deployments in response to piracy off the coast of Somalia. From a U.S. perspective, the challenge is to find a way to increase the contribu-

tions of the European partner states of NATO without demanding large, costly, and politically divisive troop deployments abroad or massive increases in defense spending. Efforts in space and cyberspace could therefore become new building blocks for effective NATO cooperation even as cooperation in traditional areas like air and sea continues. Dealing with the space and cyber issues within the confines of NATO, however, requires addressing several critical intellectual challenges.

Challenges to a Significant NATO Role in the "New" Commons

There is widespread agreement among analysts in the United States and Europe that cyberwarfare is a crucial issue for NATO; reports from the NATO-commissioned review chaired by Albright to the high-level Atlantic Council commission explicitly argue that the new NATO Strategic Concept should address cyberwarfare.[39] Secretary of State Hillary Rodham Clinton, in a speech on the future of NATO on February 22, 2010, similarly argued that NATO must work to better incorporate defenses against cyberwarfare into its expertise.[40] The United States and its NATO allies need to create a shared situational awareness of cyber security that will enable effective cooperation moving forward.

Functionally integrating cyberwarfare into NATO capabilities requires first answering some difficult questions specific to the cyber realm, including determining what types of capabilities NATO member states and NATO itself should possess. After all, most NATO activities involve coordinating the activities of NATO members, rather than developing exclusively "NATO" capabilities. The most important question is under what conditions, if any, a cyber attack on a member state or a NATO asset would trigger an Article 5 commitment for all member states to militarily rally together. There have already been real world scenarios that hint at this possibility. In May 2007, as tensions between Estonia and Russia escalated, Russia launched a massive cyber attack against Estonia that hacked into and/or disabled its government, industry, and media servers.[41] Though NATO sent experts to Estonia to help it recover from the attack and rebuild its defenses, Estonia did not invoke Article 5 and ask for a declaration of war against Russia—and it is unclear if they would have received support from much of NATO if it had.

Of special concern is the uncertainty over how to actually evaluate the damage from a cyber attack and compare it to what might have occurred in a comparable kinetic attack. As the National Academies describes with regards to cyber attacks, "collateral damage and damage assessment of a cyberattack may be very difficult to estimate."[42] Roger Cressey of Good Harbor Consulting states that given the difficulties private firms –motivated by profit—have in identifying cyber attack perpetrators at times, governments will almost certainly struggle as well.[43] Because the kinetic consequences of a cyber attack are secondary—like a UAV falling out of the sky or a power plant shutting down—creating clear and coherent standards will be tricky even if it is desirable.

One option is to lay out a specific policy that would be a part of the Strategic Concept and that describes the sort of cyber attack that is damaging enough to trigger an Article 5 commitment from other NATO member states. The risk of such a specific declaration is that it could "green light" lower level attacks by guaranteeing that they would *not* trigger a NATO response. The advantage of a specific policy is that it sets up a clear red line for potential adversaries and potentially deters more dangerous types of cyber attacks. Bureaucratically, clear guidance about responding to cyber attacks could facilitate rapid responses in a crisis and prevent dangerous delays that place the security of member states at risk. While individual NATO member states are capable of acting quickly, NATO as an institution, like many institutions, works more slowly. Having preset procedures in place to govern the response to a cyber attack could help NATO members effectively coordinate in a crisis.

Alternatively, creating a clear standard could force NATO member states into unnecessary and unwanted conflicts over unsubstantiated threats.[44] Mike Rasch, the former head of the U.S. Department of Justice's computer crimes division,

believes that the vague standards at present help members avoid being dragged into conflicts by creating "wiggle room," something that would not exist in a world of clear standards.[45]

Another approach could be to treat cyber attacks against NATO members like other types of military attacks, on a case-by-case basis. For example, the Albright report endorses decisions in each case "based on the nature, source, scope, and other aspects of the particular security challenge."[46] A loose standard could help ensure flexibility and ensure that the response is appropriate to the situation. [47] The potential downside is that confusion could result in a crisis if NATO members are not sure whether a cyber attack, already harder to "measure" than a conventional kinetic strike, was devastating enough to trigger a response.

Concerns that specific standards might drag member states into conflict are most likely overstated, as NATO members have only invoked Article 5 once, in response to the attacks on September 11, 2001. The high threshold for invoking Article 5 means countries are unlikely to do so unless they are in grave danger.[48]

One way forward might be to implement a loose standard for triggering an emergency North Atlantic Council consultation under Articles 3 and 4. Given that the treaty does not define precisely what level of conventional military attack triggers an Article 5 commitment, there is no reason cyber attacks need to be defined more specifically than other types of attacks. This sort of approach could convey to potential adversaries that NATO members take cyber attacks seriously without requiring the creation of cumbersome and time-consuming bureaucratic procedures that could bog NATO members down in definitional debates during a crisis. Eneken Tikk, a lawyer at NATO's Cyber Center of Excellence in Estonia, argues that the critical standard for evaluation is whether a cyber attack created damage comparable to a kinetic attack.[49] Measured in terms of economic losses or secondary kinetic damage caused from a cyber attack, this standard has potential to be workable and merits consideration in the Strategic Concept review. The other key cyber-related question is how to determine when NATO operations should include retaliatory cyber attacks. NATO is a defensive military alliance—Article 5 is triggered by an attack on a member state, not just a "threat." Edgar Buckley and Ioan Mircea Pascu, members of the Atlantic Council Strategic Advisors Group, argue that the upcoming Strategic Concept should not definitively resolve this issue, since setting standards at this time would be an unnecessary and hypothetical exercise in.[50] NATO members are now considering the question of preemption in general as part of the Strategic Concept review—whether a strike is justified if NATO faces an imminent military attack. The debate over preemptive cyberwarfare seems to be even more complicated.

Many countries, including the United States, are reviewing their cyber policies in an attempt to determine when, if ever, they should opt to launch retaliatory cyber operations instead of just defend themselves against cyber attacks.[51] For example, if the United States experiences a cyber attack and can trace the source, does it have the right to launch a cyber attack—or a kinetic attack—against the source? If a cyber attack were essentially equivalent to a kinetic attack, why would the rules governing those attacks differ? Launching a cyber attack could thus require the same high-level decisions and circumstances that would precede a conventional military strike.[52]

Yet, there is something different about cyber attacks, as the discussion over Article 5 and cyberwarfare illustrates. If some types of cyber attacks are less dangerous than a kinetic attack, arguably the regulations governing their use should also be looser. Speed is also a factor to consider. While some cyber attacks might take weeks or months to develop, giving NATO members ample time to consider a response strategy, others might require an immediate response, which would not only entail defending a network but would require going after the source of the attack.

Additionally, there is the question of responding to a cyber attack in kind. NATO's Computer Incident Response Capability is designed to defend NATO members from cyber attacks. If, however, a NATO member can track the specific network or IP

address of a cyber attacker, but it cannot determine whether a country or nonstate actor conducted the attack, it is unclear whether the NATO member can retaliate against the specific perpetrators. The debate over whether NATO should have a common policy or leave it to member states is political, as is the debate over whether to respond to a kinetic strike against a NATO member with a kinetic strike. Creating the capacity to coordinate national capabilities for retaliatory cyber operations within the NATO context is therefore necessary.

Even more difficult to answer is the question of when it might be appropriate to respond to a cyber attack with the use of kinetic military force. A cyber attack devastating enough to cause a country to want to respond with kinetic force using the NATO framework (as opposed to just working on its own, as Great Britain did in the Falklands) is likely to fall under the scope of attacks that could also trigger an Article 5 discussion.

Of course, NATO will never be the only actor in the cyber or space domains. In the cyber domain, for example, businesses protecting intellectual property, production processes, and other trade secrets are just as if not more interested in maintaining network security and responding to cyber attacks as governments are. Thus, NATO needs to facilitate public-private interactions to take advantage of industry expertise. While this could involve simply sharing best practices, it could also involve more robust collaboration. As long as a military is not revealing its specific methods of attack, it would likely benefit from public-private partnerships without compromising security.

Another potential challenge is engaging other international organizations and countries that wish to collaborate on cyber issues. Though there will be limits to what is possible, both cyberspace and outer space may be areas where expanding cooperation beyond NATO can yield benefits. NATO members will have their own space and cyber policies outside of the NATO context and in some situations they will cooperate with non-NATO allies as well. While collaboration with those states and organizations will be vital for a country to effectively respond to cyber and space threats at a macro level, it is unclear if NATO should push to become a global clearinghouse for more than just its members. However, active collaboration by NATO members that coordinates their cyber capabilities and develops guidance for responding to cyber attacks could help NATO serve as a larger coordinating mechanism that brings together other allied nations, such as Australia or Japan, as well.[53]

A final issue NATO must address in the context of these new threats is the national secrecy implications of integrating new technologies in the space realm. For example, the classified nature of many space technologies, since they are among the most advanced, sensitive, and vulnerable assets possessed by the United States and its allies, has hindered cooperation within NATO. NATO has operated satellites since 1970, demonstrating some capacity for action, but cooperation in the space arena is very limited.[54] U.S. Air Force Lt. Colonel Tom Single, deployed in Kabul in 2009–2010 with ISAF, recently argued that secrecy between NATO members concerning space assets actively hinders ISAF's efforts in Afghanistan.[55]

Single identified two key issues for future NATO efforts involving space. First, NATO's European member states have not systematically integrated potential space assets into their operational concepts. This often places them at a disadvantage compared to the United States—and sometimes even compared to insurgents. Second, classification issues prevent NATO allies from sharing information, especially in real-time, with each other. U.S. Army General David Petraeus argues that these barriers between allies make cooperation significantly more difficult and less effective.[56] As Single writes:

> Due to classification levels, we can't share this with 44 nations, so we often worked these issues behind closed doors…Over-classification and releasability are the No. 1 challenges. Sometimes, just because a piece of information came from a space system, it was marked 'Secret.' And this is true not only of U.S. systems but of others as well.[57]

A European defense official recently verified Single's point about the problem not being uniquely American. The official said, "Military satellites in Europe are designed for use only by the nation that owns the asset, or at best for bilateral use as part of an exchange agreement with another nation."[58]

Protecting the "New" Commons: An Opportunity for NATO?

How can NATO work to address these new challenges to the global commons given the potential impediments to cooperation? In the cyber arena, all NATO members should recognize the vital importance of increasing the security of the commons. If they do, NATO may more easily get "buy in" from members otherwise unwilling to spend additional resources on national security. Since secure communications through cyberspace are absolutely necessary for global commerce, they are critical to the economies of every major European nation. Dominance over the cyber domain is also currently in flux, as no state has overwhelming capabilities. The relative impact of coherent action by the European member states of NATO could therefore offer larger "bang for the buck" than investments in more established military arenas. Other elements of cyberspace also make it a very attractive area for European militaries and governments to address. Lacking a constant geographic address, cyberspace naturally transcends national borders, requiring international solutions that should draw the attention of European states interested in international law and the enforcement of international norms. Working together, the United States and its NATO allies could become norm entrepreneurs with their cyber policies, serving as role models for other Western allies and democracies as they attempt to handle the national security implications of cyberspace.

Cyberspace thus probably offers the greatest potential for renewed NATO action in the commons. It is an area where NATO authorities have already demonstrated interest. At the 2002 Prague Summit, NATO members declared cyber security to be an important issue. In 2008, partially in response to the 2007cyber attacks against Estonia, NATO established the Cyber Defence Management Authority (CDMA) to coordinate NATO's cyber-response policies.[59] NATO also has an Information Assurance Technical Center and a Center of Excellence for Cyber Defense (CCDC).[60] At the 2008 NATO Summit in Bucharest, the official summit declaration stated:

> NATO remains committed to strengthening key Alliance information systems against cyber attacks. We have recently adopted a Policy on Cyber Defence, and are developing the structures and authorities to carry it out. Our Policy on Cyber Defence emphasizes the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack. We look forward to continuing the development of NATO's cyber defence capabilities and strengthening the linkages between NATO and national authorities.[61]

Unfortunately, the function and role of the CDMA remains unclear, as does the role of cyber security for many NATO countries. The United States is committed to robust cyber investments and is working on creating a coherent, whole-of-government cyber policy, including a declaratory policy to govern the way the United States will respond to cyber attacks.[62] In addition, not all NATO member states share this sense of urgency. In 2009, for example, Great Britain's government acknowledged that it still lacked a coherent cyber security budget within its Ministry of Defence.[63]

As part of engaging in extensive, high-level consultation with NATO allies on cyber security, the United States should consider the following actions within the NATO architecture:[64]

First, NATO now has several different cyber warfare related organizations, including the CDMA, CCDC, and the Computer Incident Response Center (CIRC). While all technically dis-

tinct and based in different locations, this type of bureaucratic overlap could cause organizational confusion. NATO members should consider consolidating these organizations into a single, unified command to better facilitate the integration of cyberwarfare within NATO.

Second, recognizing the difficulties in measuring the "costs" of a cyber attack, NATO members should consider adopting a loose equivalence standard whereby a cyber attack has to reach the levels of a kinetic attack that would be considered sufficient to trigger Article 5. This agreement would not necessarily require public documentation—or formal signature—but NATO members nonetheless should reach an understanding on the issue.

Third, support should be increased for NATO's CCDC on the condition that it is required to study retaliatory cyber operations. Currently, the CCDC lacks coordinated, long-term funding and defensive efforts encompass much of its work, due to NATO's existing experiences with cyber attacks. The CCDC should also conduct research and evaluate feasible and calculated responses in the case of a strategic cyber attack.

Fourth, NATO member governments should reach out to private industry, especially in Canada, Europe, and the United States where there is direct economic interest in cyber security. Cyber security is one area where market forces may drive a "race to the top." The United States should encourage regular, cross-national dialogue between corporate cyber security leaders and NATO to exchange best practices. Finally, NATO member states should consult with private industry leaders to create design metrics for the consequences of cyber attacks. Since they already have to monetize the cost of attacks for shareholders, private corporations may have insights for governments.

NATO should also respond to the challenges it faces in outer space. As Canadian Lt. Colonel Jim Bates argues, space is a "critical enabler of NATO operations."[65] Unfortunately, in contrast to cyberspace, outer space has received less high-level attention within NATO. For example, while high-level NATO publications on NATO's strategy published between 1991 and 2006 mention air power, sea power, and cyberwarfare, space is tellingly absent from most documents.[66] There is no high-level NATO guidance concerning space. The 2009 Joint Air Power Competence Center's (JAPCC) Space Operations Assessment concludes, "The current approach to Space is piecemeal, a bottom-up effort lacking overarching structure or direction. While this may have been adequate in the past, the complexities of modern security challenges demand a more deliberate approach to Space."[67]

One potential reason for the lack of NATO guidance regarding space is that while space has already been militarized—meaning many nations use space assets to facilitate military operations—space has not yet been weaponized—meaning no nation deploys weapons in space. The lack of space weaponization may decrease the perceived urgency for NATO to address outer space. Additionally, while the EU backed down from its attempt to explicitly supplant the U.S.-initiated and controlled global positioning system (GPS) with its own Galileo satellite architecture, the EU's Galileo system will be a commercial alternative to GPS.[68] In early 2010, the European Space Agency signed three contacts designed to create the first stage of the Galileo system.[69] These trends could theoretically disincentivize NATO member states from cooperating with the United States in space, since they may believe they will soon free themselves from dependence on U.S. space assets. Increased European satellite capabilities, however, should lead to more coordination with the United States. The European Parliament's statement on February 19, 2009 on the European Security Strategy and the European Security and Defence Policy also recognizes the potential military relevance of Galileo. Item number fifty of the statement clearly states that the European Parliament "Considers it necessary to allow the use of the Galileo and GMES (Global Monitoring for Environment and Security) systems for security and defence purposes."[70]

These ambitions, however, have not yet translated into greater military space awareness on the part of the European member states. Richard McKinney, the European Space Liaison at the Office of the Undersecretary of the U.S. Air Force,

argues that the lack of European space capabilities explains much of the secrecy on the U.S. side.[71] After all, if the United States does not have a great deal to gain from sharing its space secrets with its European partners, it lacks the incentive to cooperate.

The need to protect existing space assets should provide the incentive NATO members need to cooperate. An estimate by the Organization for Economic Cooperation and Development places the replacement cost of global space assets at $230 billion dollars.[72] Space is also an important future theater for all NATO member states. Whether or not they are directly involved in a given conflict, all NATO states have important economic interests in secure space access. Another incentive is the need for redundancy given the vulnerability of space assets. The ability to draw easily and quickly on the space assets of allies across NATO could help all member states in a crisis if a cyber attack or anti-satellite weapon disrupts one state's access to satellite information.[73]

One area for potential future collaboration is the Eagle Vision I effort. During the first Gulf War, in response to the need for rapid updates about events on the ground, France cooperated with the United States to build the world's first mobile image processing unit. Since then, utilizing France's SPOT satellites, the United States and France have cooperated to produce real-time satellite imagery in emergencies such as Hurricanes Katrina and Rita.[74]

Thus, the United States should consider exploring the following measures to clarify NATO's role in space. First, the United States should assist the JAPCC in its recommendation to establish a NATO Space Command within NATO headquarters to facilitate multinational space cooperation in peacetime and crisis situations.[75] Such an effort would provide an easy mechanism for real time information sharing. It would also represent recognition of the space challenge by NATO, which has commands in other areas of the commons. The command could also facilitate cooperation in dealing with space debris, a constant threat to both commercial and military satellites. Second, NATO should create cooperative space training exercises just as the United States and its allies do in the air realm with exercises like "Red Flag." Creating yearly cooperative space training exercises to help improve interoperability and mutual understanding will help NATO become more effective in the space realm.[76] Third, the United States should urge NATO to consider creating a "space liaison" or similar position to facilitate real-time sharing of intelligence information collected from space assets by ISAF partners in Afghanistan.

Whether these recommendations prove realistic and valuable may depend more on the European member states of NATO than on the United States. Commercially and militarily, U.S. engagement with space will only deepen over the next few decades. Other NATO member states need to consider the relevance of space to their commercial and security interests and consider these measures as first steps to ensure a role for NATO in space. The alternative is an ad-hoc relationship between the United States and European Space Agency that will likely be less effective and useful for both sides than an institutionalized relationship forged through NATO.

Protecting the "Traditional" Commons: Does NATO Still Have a Role?

Of course, cyberspace and outer space are not the only areas of the commons where NATO will operate over the next generation. NATO already operates in the air and at sea, which are known as the "traditional" areas of the global commons. Due to the financial requirements to generate significant new air and sea capabilities, however, cooperation between the United States and its NATO allies in these areas of the commons will be limited to building on existing capabilities.[77] This could make it increasingly hard to use NATO resources for military operations in the air and sea, though deep cooperation will still exist in areas like protection from piracy.

Naval Power

The oceans of the world are the best- and longest-studied part of the global commons.[78] They are also still crucial to the global economy and global stability. The UN Conference on Trade and Development recently stated that over 8 billion tons of goods were transported on the sea in 2008.[79] Other studies have estimated that 70–90 percent of global commerce occurs in the oceans .[80] The naval domain is also one of the best-established areas for cooperation within NATO. NATO has included robust naval operations since its inception, but its overall capabilities in the seas rely heavily on the vast forces possessed by the United States. With eleven carrier groups and an unmatched submarine force, the United States has exercised command of the naval commons since the end of World War II.[81] For the last sixty years, potential adversaries to the United States have overwhelmingly chosen to counter U.S. surface naval superiority by developing anti-access forces like submarines, land-based naval aircraft, and submarines rather than to confront the United States directly.

This equation may be changing, however, due to the rapid expansions of both the Chinese and Indian navies over the last several years.[82] The spread of advanced anti-access technologies like quiet diesel submarines may also mean that many more nations can threaten U.S. naval forces intent on projecting power into a given region. The result, according to experts like Andrew Krepinevich of the Center for Strategy and Budgetary Assessments, is a potentially large-scale challenge to U.S. control of the naval commons.[83]

The naval arena features some of the most tangible examples of specialization by NATO member countries to complement U.S. power. NATO member states with expertise in counter-mine operations and anti-submarine warfare participate in regular military exercises alongside the U.S. Navy. The Netherlands and Belgium, for example, host NATO's center of excellence for naval mine warfare.[84]

NATO members have prominently deployed naval forces over the last few years to counter the renewed risk of piracy in the Gulf of Aden, off the coast of Somalia. Anti-piracy operations are another example of specialization within NATO: while the European member nations of NATO lack the ability, for the most part, to project significant naval power over large distances without the assistance of the United States, they do have sufficient naval assets to conduct anti-piracy operations.[85] In September 2007, ships from six NATO nations began patrolling the Somali coast to search for pirates.[86] NATO then implemented Operation Allied Provider from October to December 2008, Operation Allied Protector from March to August 2009, and finally Operation Ocean Shield in August 2009, which is currently ongoing. Ships from the Royal Navy, Greek navy, Italian Navy, Turkish Navy, and U.S. Navy currently participate in Operation Ocean Shield.[87]

Anti-piracy operations are a measurable indicator of the ability of NATO members to operate together and successfully deploy military force beyond NATO's borders. Even the anti-piracy arena, however, is not without challenges. For example, in addition to NATO's ongoing anti-piracy deployments, EU member states have deployed assets to the Gulf of Aden as part of Operation ATALANTA.[88] Yet unresolved is whether NATO's European members are more bound by EU regulations or NATO regulations. If the two come into conflict, as is possible when dealing with complicated international legal questions concerning how to handle pirates captured at sea, no governing body or principle exists to determine what policy to implement. Moving forward, NATO members need to be able to maintain an independent operational posture when some of the same members are also deploying naval assets through the EU.

In terms of more traditional naval operations, the construction of new aircraft carriers by France and Great Britain suggests that some of the European member states of NATO will have the ability to project naval power over the next generation. This could change, as budgetary pressures are forcing Great Britain to revise its carrier construction plans, but even new smaller carriers will renew the Royal Navy's capacity to project power

and exercise sea control in collaboration with the U.S. Navy.[89]

The naval commons are therefore an area where NATO cooperation is already institutionalized and likely to continue in the future. There are some risks, of course. Declining European defense budgets could undermine the ability of a growing number of NATO members to participate in maritime operations. Since conventional naval battles involving NATO seem unlikely to occur in the near-term, the atrophying of traditional European naval capabilities is unlikely to have a substantive impact on the global naval balance. However, NATO's European member states should invest more robustly not just in their own direct naval security needs, but also to keep the U.S. Navy committed to NATO.

Air Power

A litany of international agreements governs civilian air traffic and establishes rules for military aircraft in situations short of war. Control of the air enables a variety of NATO missions, including search and rescue and supply deliveries, in addition to traditional military strikes. Since the end of the Cold War, NATO forces have enjoyed air superiority in every theater where they have engaged. Much of this advantage is due to U.S. forces, though other NATO member countries have powerful air forces as well. Control of the air is vital to NATO operations—some NATO operations, such as the intervention in Kosovo, were initially waged entirely from the air. Air superiority is also a necessary prerequisite to conducting COIN operations and protecting NATO interests on the oceans. NATO's 1991 Strategic Concept, which described NATO's role in the post–Cold War world, pointed to air power as a critical area for investment by member states.[90] In 2005, to conceptualize the future of air and space forces within the NATO context, NATO created the JAPCC.[91] Air Commodore Garfield Porter, assistant director of transformation at the JAPCC, argues that air power has been essential to gaining an asymmetric advantage over the Taliban in Afghanistan, both in terms of kinetic operations and intelligence gathering.[92]

Yet, control of the air is no longer considered a priority by some of the European members of NATO. For example, a February 19, 2009 European Parliament resolution on the future of European security listed cyber space, outer space, and the oceans as important areas of interest, but did not mention the skies.[93] Air power is also absent from the 2003 European Security Strategy statement published by the EU.[94] Combined with the declines in European defense spending described above, trends in air power suggest that NATO members may face hurdles if they seek to collaborate in the air commons in situations where NATO forces lack complete air superiority.

There are several areas where the United States and its NATO allies might still be able to cooperate to increase NATO's collective air power beyond the simple aggregate of U.S. air power and the power of its allies. As the discussion above suggests, however, air power is not an area where the United States' European allies are likely to perceive significant threats requiring the investment of new resources. Thus, the most direct action could involve a relatively new area of air power— UAVs. Since the role of UAVs in the future of warfare is less settled, the opportunities for cooperation may be greater. More complete adoption of the JAPCC "Strategic Concept For Employment Of Unmanned Aerial Systems"[95] may aid in those efforts. Furthermore, it is imperative to focus on implementing STANAG 4586, the NATO-wide standards for UAV development to ensure future interoperability and allow for joint ventures when appropriate given financial and national security concerns. Finally, sharing of air assets in ISAF operations between the United States and its allies should increase to include more cooperative activities between U.S. air assets and NATO ground forces.

Conclusion

NATO has been a force for regional and global stability since its inception in the early years of the Cold War, but divergent threat perceptions between the United States and. its European allies, as well as within Europe, currently present a large-scale

challenge to NATO's relevance. The growing insecurity of the global commons makes addressing NATO's future all the more important. Protecting those areas of the globe that are beyond immediate sovereign control is necessary for the stable functioning of the global economy and security in every region of the world.

Cyberspace holds the most promise for new NATO cooperation in the commons. Even if some European members of NATO do not view air and sea threats as likely to emerge in the near to medium term, NATO members such as Estonia are already painfully aware of the consequences of cyberwarfare. Expanded cyber cooperation is a tangible area where NATO members can work together to build expertise that will protect NATO members from attack and generate the capability to effectively launch attacks when necessary.

NATO members still need to work out key issues, especially in order to determine when a cyber attack would trigger Article 5 obligations and when offensive cyber operations are justified. Recognizing that cyberwarfare will not be a purely defensive action for NATO states is absolutely crucial. By orienting its cyber operations entirely around defenses, NATO risks creating an alliance-wide "Maginot Line" that increases the vulnerability of all NATO members.[96]

The space commons have lain dormant, in a regulatory sense, since the 1960s. With the European Galileo satellite constellation nearing takeoff, NATO should focus anew on space cooperation. Every NATO country relies on safe and reliable access to space assets for both commerce and military operations. Ensuring redundancy and the interchangeability of space assets in a crisis, along with enhancing real-time sharing of satellite data in places like Afghanistan, are ways NATO can work together in the space commons.

Finally, by using the naval assets it does have, NATO is already playing a critical role in reducing incidences of piracy in the Gulf of Aden. The navies possessed by the United States' European partners in NATO are actually well-suited to these sorts of tasks. The original reason that bound the member states of NATO together—Soviet threat—no longer exists. NATO, however, still has a role to play in ensuring global stability. Given obvious constraints, it is crucial to not let expectations about NATO's future become unrealistic. However, by enhancing its role in some specific areas of the global commons, NATO can continue to play a vital part in ensuring regional and global stability for the next generation.

About the Project

The Transatlantic Paper Series is a product of The Chicago Council on Global Affairs' project on "The Future of the Transatlantic Alliance in a Changing Strategic Environment." The project seeks to identify ways in which the United States and Europe can deepen cooperation and maintain collective influence as the geopolitical center of gravity moves toward Asia and the Middle East. In addition to the paper series, the project includes a final report entitled "The Transatlantic Alliance in a Multipolar World," authored by Thomas Wright and Richard Weitz. Over the past year, project activities have included workshops, conferences in the United States and Europe, and research trips to Asia and Europe. The project was made possible by generous funding from the Robert Bosch Stiftung, the McCormick Foundation, and the Adenauer Fund at The Chicago Council on Global Affairs. All views and opinions expressed in the papers are those solely of the authors. The Chicago Council takes no institutional position on policy issues and has no affiliation with the U.S. government. All statements of fact and expressions of opinion contained in this paper are the sole responsibility of the author and may not reflect the views of his respective organization or the project funders.

Notes

1 See Office of the Secretary of Defense, U.S. Department of Defense, "Quadrennial Defense Review Report," February 2010, p. xiv, http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf (hereinafter 2010 Quadrennial Defense Review) and Abraham M. Denmark and James Mulvenon, eds., "Contested Commons: The Future of American Power in a Multipolar World," January 2010, http://www.cnas.org/files/documents/publications/CNAS%20Contested%20Commons_1.pdf.

2 See NATO, "NATO's New Strategic Concept," Web site, 2010, http://www.nato.int/strategic-concept/index.html.

3 NATO, "NATO operations and missions," September 17, 2010, http://www.nato.int/cps/en/natolive/topics_52060.htm.

4 Ivo Daalder and James M. Goldgeier, "Global NATO?," *Foreign Affairs* 85, no. 5 (September/October 2006): 105.

5 Robert M. Gates, remarks, NATO Strategic Concept Seminar, National Defense University, Washington, D.C., February 23, 2010, http://www.defense.gov/speeches/speech.aspx?speechid=1423 (hereinafter Gates' remarks).

6 See Madeleine K. Albright, "NATO 2020: Assured Security; Dynamic Engagement," May 17, 2010, p. 38, http://www.acus.org/files/publication_pdfs/3/NATO2020-Experts-Report.pdf.

7 Data taken from International Institute for Strategic Studies, *The Military Balance* (London: Routledge, 2010). Accessed online on May 8, 2010.

8 See Gates' remarks. He was echoing President Barack Obama's speech accepting the Nobel Peace Prize on December 10, 2009. Obama stated that while the United States still viewed some values as worth the use of military force, he worried that some of the United States' European allies no longer felt the same way. See Office of the Press Secretary, The White House, "Remarks by the President at the acceptance of the Nobel Peace Prize," Oslo, Norway, December 10, 2009, http://www.whitehouse.gov/the-press-office/remarks-president-acceptance-nobel-peace-prize.

9 Julian Lindley-French and Yves Boyer, "STRATCON 2010: An Alliance for a Global Century," April 2010, p. 5, http://acus.org/files/publication_pdfs/3/STRATCON%202010%20REPORT_FINAL.pdf.

10 According to Jackson Janes, executive director of the American Institute for Contemporary German Studies at the Johns Hopkins University in Washington, D.C., this gap poses an enormous test for NATO. See Jackson Janes, "Alliance Asymmetries," March 4, 2010, http://www.aicgs.org/analysis/at-issue/ai030410.aspx.

11 See Robert Marquand, "Dutch government collapse: Will other European troops now leave Afghanistan?" *Christian Science Monitor*, February 22, 2010, http://www.csmonitor.com/World/2010/0222/Dutch-government-collapse-Will-other-European-troops-now-leave-Afghanistan.

12 See Zaki Laidi, "Europe As A Risk Averse Power: A Hypothesis," *Gannett Policy Brief*, no. 11 (February 2010), http://www.laidi.com/sitedp/default/files/file/GARNET11-COR-WEB.pdf.

13 Albright, "NATO 2020: Assured Security; Dynamic Engagement," p. 17.

14 See Lindley-French and Boyer, "STRATCON 2010: An Alliance for a Global Century," pp. 5-6.

15 Alfred T. Mahan, *The Influence of Sea Power Upon History, 1660–1783* (Mineola, NY: Dover Publications, November 1987).

16 This paper focuses on areas of the commons and per se and, as such, does not discuss issues arising from the potential deployment of missile defense systems. A great wealth of literature on missile defense systems already exists and focusing on it in this context might distract from the broader point.

17 NATO's Allied Transformation Command has recognized the importance of the global commons and is now beginning to convene conferences and workshops on the issue. See http://www.act.nato.int/globalcommons.

18 William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber attack Capabilities* (Washington, D.C.: National Academies Press, 2009), p. 162.

19 Thanks to Abe Denmark of the Center for New American Security for pointing this out.

20 For example, see John Arquilla and David F. Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: RAND Corporation, 1996); John Arquilla and David F. Ronfeldt, *The Emergence of Noopolitik: Toward an American Information Strategy* (Santa Monica, CA: RAND, 1999); John Arquilla and David F. Ronfeldt, *Swarming & the Future of Conflict* (Santa Monica, CA: RAND, 2000); John Arquilla and David F. Ronfeldt, eds., *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001).

21 See 2010 Quadrennial Defense Review, p. 2. Also, see U.S. Department of Defense, "National Defense Strategy," June 2008, p. 1, http://www.defense.gov/news/2008%20National%20Defense%20Strategy.pdf.

22 Owens, Dam, and Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber attack Capabilities*, p. 122.

23 Ibid., p. 7.

24 See John J. Kruzel, "Cybersecurity Seizes More Attention, Budget Dollars," American Forces Press Service, February 4, 2010, http://www.defense.gov/news/newsarticle.aspx?id=57871.

25 See Larry M. Wortzel, Testimony before Committee on Foreign Affairs, House of Representatives, "China's Approach to Cyber Operations: Implications for the United States," March 10, 2010. http://www.internationalrelations.house.gov/111/wor031010.pdf.

26 This list excludes cyber attacks viewed as more exclusively oriented toward commercial entities. One example of such an attack is the recent accusation by Google of systematic Chinese efforts to infiltrate the computer systems of foreign companies operating in China. Andrew Jacobs, "Google, Citing Attack, Threatens to Exit China," *New York Times*, January 20, 2010, http://www.nytimes.com/2010/01/13/world/asia/13beijing.html.

27 See John Markoff, "Before the Gunfire, Cyber attacks," *New York Times*, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html.

28 See Mike Harvey, "Chinese hackers 'using ghost network to control embassy computers'," *TimesOnline*, March 30, 2009, http://www.timesonline.co.uk/tol/news/uk/crime/article5996253.ece.

29 See "Estonia hit by 'Moscow cyber war'," *BBC News*, May 17, 2007, http://news.bbc.co.uk/2/hi/europe/6665145.stm.

30 See Nathan Thornburgh, "The Invasion of the Chinese Cyberspies," *Time*, August 29, 2005, http://www.time.com/time/magazine/article/0,9171,1098961,00.html. Based on the National Academies distinction between cyber attack and cyber espionage, many existing Chinese efforts may be better classified as cyber espionage rather than cyber attack. Regardless, it is important to design defenses against them. See Owens, Dam, and Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber attack Capabilities*, p. 18.

31 For a similar take that also discusses the large challenges involved in deterring cyber attacks, see Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), p. xvi. Libicki concludes that defending cyber networks should remain the primary role of US cyber assets, though developing some warfare capabilities is necessary as well.

32 See William F. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010), pp. 97–108, 99–100.

33 For more on this in relation to cyber deterrence in general and the case of Estonia, see Will Goodman, "Cyber Deterrence: Tougher in Theory than in Practice," *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 102–135, 105.

34 See Chris Demchak, "Conflicting Policy Presumptions about Cybersecurity: Cyber-Prophets, -Priests, -Detectives, - and Designers, and Strategies for a Cybered World," 2010, http://www.acus.org/files/publication_pdfs/403/Demchak-brief.pdf.

35 See Thomas Single, "Considerations for a Nato Space Policy," *European Space Policy Institute Perspectives*, no. 12 (September 2008), http://www.espi.or.at/images/stories/dokumente/studies/espi_perspectives_12.pdf and Air Commodore Jan A.H. van Hoof, "Coalition Space Operations - a Nato Perspective," *HIgh Frontier: The Journal for Space and Cyberspace Professionals* 6, no. 2 (February 2010): 10, http://www.afspc.af.mil/shared/media/document/AFD-100226-085.pdf.

36 See Eric Sterner, "Beyond the Stalemate in the Space Commons," in "Contested Commons: The Future of American Power in a Multipolar World," eds. Abraham M. Denmark and James Mulvenon, p. 108.

37 See Phillip C. Saunders, "China's Future in Space: Implications for U.S. Security," *adAstra: The Magazine of the National Space Society*, Spring 2005, http://www.space.com/adastra/china_implications_0505.html.

38 See Craig Covault, "Chinese Test Anti-Satellite Weapon," *Aviation Week & Space Technology*, January 17, 2007, http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=space&id=news/CHI01177.xml.

39 See Albright, "NATO 2020: Assured Security; Dynamic Engagement" and Lindley-French and Boyer, "STRATCON 2010: An Alliance for a Global Century."

40 See Hillary Rodham Clinton, *NATO's Future: Speech before the Atlantic Council*, February 22 2010 (Washington, DC, http://www.acus.org/event/hillary-clinton-future-nato/transcript.

41 See Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian*, May 17, 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

42 Owens, Dam, and Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber attack Capabilities*, p. 81.

43 See Bob Sullivan, "Could cyber skirmish lead U.S. to war?" The Red Tape Chronicles, MSNBC.com, June 10, 2010, http://redtape.msnbc.com/2010/06/imagine-this-scenario-estonia-a-nato-member-is-cut-off-from-the-internet-by-cyber-attackers-who-besiege-the-countrys-bandw.html.

44 In international relations, this process is called "chain-ganging." See Thomas J. Christensen and Jack Snyder, "Chain gangs and passed bucks: predicting alliance patterns in multipolarity," *International Organization* 44, no. 2 (March 1990): 137–168.

45 See Sullivan, "Could cyber skirmish lead U.S. to war?"

46 Albright, "NATO 2020: Assured Security; Dynamic Engagement," p. 20.

47 See Edgar Buckley and Ioan Mircea Pascu, "Article 5 and Strategic Reassurance," 2010 February, http://www.acus.org/files/publication_pdfs/403/Article5_SAGIssueBrief.PDF.

48 On the other hand, an unclear, case-by-case standard could risk a member state invoking Article 5 and having other NATO members refuse to participate. Independent of the specific situation, such an event—though unlikely— would dramatically undermine NATO's credibility moving forward.

49 See Michael Smith and Peter Warren, "Nato warns of strike against cyber attackers," *The Sunday Times*, June 6, 2010, http://www.timesonline.co.uk/tol/news/world/article7144856.ece.

50 See Buckley and Pascu, "Article 5 and Strategic Reassurance," p. 3.

51 This is critical. Without coherent cyber policies articulated by the United States and other NATO members, collaboration within NATO will become more difficult. See Office of the Press Secretary, The White House, "Remarks by the President on Security our Nation's Cyber Infrastructure," May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ and Tom Gjelten, "Cyber attack: U.S. Unready for Future Face of War," National Public Radio, April 7, 2010, http://www.npr.org/templates/story/story.php?storyId=125598665.

52 See Owens, Dam, and Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber attack Capabilities*, pp. 80–82.

53 One topic worth exploring is using the protection of the cyber commons as a means to engage India.

54 See van Hoof, "Coalition Space Operations - A NATO Perspective," p. 10.

55 See Peter B. de Selding, "U.S. Officer: Secrecy Among Coalition Forces Hinders Use of Space Assets in Afghanistan," *Space News*, May 7, 2010, http://www.spacenews.com/military/100507-secrecy-space-assets.html.

56 See Christopher P. Cavas, "Petraeus: U.S. must share more info with allies," *Air Force Times*, May 12, 2010, http://www.airforcetimes.com/news/2010/05/military_petraeus_sharing_intel_051210w/.

57 Quoted in de Selding, "U.S. Officer: Secrecy Among Coalition Forces Hinders Use of Space Assets in Afghanistan."

58 Ibid.

59 An official description of NATO's evolving cyber-response policy is available at NATO, "Defending against cyber attacks," Web site, September 16, 2010, http://www.nato.int/cps/en/natolive/topics_49193.htm.

60 On NATO's technical computer assurances, see NATO Computer Incident Response Capability, Web site, http://www.ncirc.nato.int/. For the homepage of the Cyber Defense Center of Excellence in Estonia, see Cooperative Cyber Defence Center of Excellence, Web site, http://www.ccdcoe.org/.

61 NATO, "Bucharest Summit Declaration," press release, April 3, 2008, http://www.nato.int/cps/en/natolive/official_texts_8443.htm?mode=pressrelease.

62 See The White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," June 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

63 See "MoD cyber security budget unclear," Defencemanagement.com, April 24, 2009, http://www.defencemanagement.com/news_story.asp?id=9281.

64 See Owens, Dam, and Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber attack Capabilities*, pp. 59–60.

65 See Lieutenant Colonel Jim Bates, "JAPCC: Joint Air Power Competence Centre: NATO's Centre of Excellence," *Canadian Air Force Journal* 1, no. 2 (Summer 2008): 56. http://www.airforce.forces.gc.ca/CFAWC/eLibrary/Journal/Vol1-2008/Iss2-Summer/AF_JOURNAL-Vol1-2008-Iss2-Summer_e.pdf.

66 See NATO, "Toward The New Strategic Concept: A selection of background documents," 2010, http://www.nato.int/ebookshop/stratcon/off-text-e.pdf.

67 See Thomas Single, "NATO Space Operations Assessment," January 2009, p. 1, https://transnet.act.nato.int/WISE/NATOSpaceO/file/_WFS/NATO%20Space%20Ops%20Assessment%20Jan%2009.pdf.

68 See Richard W. McKinney, "Military International Space Cooperation," *HIgh Frontier: The Journal for Space and Cyberspace Professionals* 6, no. 2 (February 2010): 4. http://www.afspc.af.mil/shared/media/document/AFD-100226-085.pdf.

69 See European Space Agency, "Major Galileo contracts signed," *European Space Agency News*, January 27, 2010, http://www.esa.int/esaCP/SEMPX0SJR4G_index_0.html.

70 European Parliament, "Resolution of 19 February 2009 on the European Security Strategy and ESDP," February 19, 2009, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0075+0+DOC+XML+V0//EN.

71 See McKinney, "Military International Space Cooperation," p. 3.

72 See Organization for Economic Co-Operation and Development (OECD), *The Space Economy at a Glance 2007* (Paris: OECD, 2007).

73 See McKinney, "Military International Space Cooperation," p. 5.

74 Ibid., p. 4.

75 Single, "NATO Space Operations Assessment."

76 See McKinney, "Military International Space Cooperation," p. 5.

77 This presumes the security environment is relatively static and no large-scale conventional military threat to the European NATO states emerges.

78 Oldest in that they have been utilized for the longest period of time.

79 See UN Conference On Trade And Development (UNCTAD), "Review of Maritime Transport 2009," 2009, http://www.unctad.org/en/docs/rmt2009_en.pdf.

80 See International Maritime Organization, Maritime Knowledge Center, "International Shipping and World Trade Facts and Figures," October 2009, http://www.imo.org/includes/blastDataOnly.asp/data_id%3D28127/InternationalShippingandWorldTrade-factsandfiguresoct2009rev1___tmp65768b41.pdf.

81 See Barry Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security* 28, no. 1 (Summer 2003): 5–46.

82 See Robert D. Kaplan, "The Geography of Chinese Power," *Foreign Affairs* 89, no. 3 (May/June 2010): 22–41.

83 See Andrew F. Krepinevich Jr., "The Pentagon's Wasting Assets: The Eroding Foundations of American Power," *Foreign Affairs* 88, no. 4 (July/August 2009): 18–35.

84 See Belgian-Netherlands Naval Mine Warfare School, Web site, http://www1.eguermin.org/.

85 One challenge, however, has been how to deal with the pirates the NATO forces catch. A patchwork of national legal opinions concerning the status of the pirates means they are released from custody as often as they are placed into more permanent custody or shipped to Kenya for trial. See Douglas Guilfoyle, "Counter-Piracy Law Enforcement And Human Rights," *International and Comparative Law Quarterly* 59, no. 1 (January 2010): 141–169.

86 See Nick Childs, "NATO show of strength off Somalia," *BBC News*, September 21, 2007, http://news.bbc.co.uk/2/hi/africa/7007778.stm.

87 These ships are part of SNMG2, one of NATO's rapid response maritime units. For more information on these piracy operations, see NATO, "Counter-piracy," September 16, 2010, http://www.nato.int/cps/en/natolive/topics_48815.htm.

88 For more on the EU mission see EUNAVFOR Somalia, Web site, http://www.eunavfor.eu/about-us/mission/.

89 See Amy Wilson, "Can Britain afford not to build £5bn Royal Navy aircraft carriers?" *The Daily Telegraph*, February 28, 2010, http://www.telegraph.co.uk/finance/newsbysector/industry/7338842/Can-Britain-afford-not-to-build-5bn-Royal-Navy-aircraft-carriers.html.

90 For NATO's Strategic Concept of 1991, see NATO, "Toward The New Strategic Concept: A selection of background documents," p. 30. http://www.nato.int/ebookshop/stratcon/off-text-e.pdf.

91 See Joint Air Power Competence Center (JAPCC), Web site, http://www.japcc.de/.

92 See Paul French, "Nato at 60: What next for air power?" airforce-technology.com, March 4, 2009, http://www.airforce-technology.com/features/feature50498/.

93 See European Parliament, "Resolution of 19 February 2009 on the European Security Strategy and ESDP". http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0076+0+DOC+XML+V0//EN.

94 See EU, "A Secure Europe In A Better World," December 12, 2003, http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf.

95 See JAPCC, "The Joint Air Power Competence Centre Strategic Concept Of Employment For Unmanned Aircraft Systems In NATO," January 4, 2010, http://japcc.de/fileadmin/user_upload/projects/nato_flight_plan_for_uas/NATO_UAS_CONEMP_Final.pdf.

96 General James Cartwright has made similar comments in terms of the United States. See Owens, Dam, and Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber attack Capabilities*, p.162.

The Chicago Council on Global Affairs Transatlantic Paper Series

Counterinsurgency and the Future of NATO by John Nagl and Richard Weitz

U.S.-EU Partnership and the Muslim World: How Transatlantic Cooperation Will Enhance Engagement by Emile Nakhleh

A Common Future? NATO and the Protection of the Commons by Michael Horowitz

NATO's Nonproliferation Challenges in the Obama Era by Richard Weitz

Also see:
The Transatlantic Alliance in a Multipolar World by Thomas Wright and Richard Weitz

For more information, visit www.thechicagocouncil.org

About The Chicago Council on Global Affairs

The Chicago Council on Global Affairs is a leading independent, nonpartisan organization committed to influencing the discourse on global issues through contributions to opinion and policy formation, leadership dialogue, and public learning.

The Chicago Council provides members, specialized groups, and the general public with a forum for the consideration of significant international issues and their bearing on American foreign policy. In addition to remaining the premier platform in the Midwest for international leaders in foreign policy, The Chicago Council strives to take the lead in gaining recognition for Chicago as an international business center for the corporate community and to broaden and deepen The Chicago Council's role in the community.

The Chicago Council takes no institutional position on policy issues and has no affiliation with the U.S. government. All statements of fact and expressions of opinion contained in this paper are the sole responsibility of the author and may not reflect the views of his respective organization or the project funders.

332 South Michigan Avenue
Suite 1100
Chicago, Illinois 60604-4416
T 312.726.3860
F 312.821.7555
thechicagocouncil.org