HARVARD IOP

National Security in Cooperation

POLICY BRIEF

May 2014

The United States, the United Kingdom, and International Actors

Authors

LEE MORROW, CHAIR
ANTHONY RAMICONE, CHAIR
CAROLINE WILLIAMS
SPENCER GISSER
MICHAEL RAYNIS
MICAELA PACHECO CEBALLOS
JONAH SALTZMAN
ELSA KANIA
BENJAMIN BETIK
MICHAEL O'BRIEN
ANDREA COOPER
WRIGHT SMITH
BLAKE MCGHGHY
ALEXANDRA SKOLER
SHAWHEEN REZAEI
JUSTINE FERRY
AARON KANZER
ADAM HOTCHKISS
AVIKA DUA
JENNIFER WALSH
ANASTASIA MORAN
NISREEN SHIBAN
WILLIAM GREENLAW
VANESSA GONZALEZ LOPEZ
PETER DELLA ROCCA

Table of Contents

Cover Pictures: US/UK flage retreived from Reuters (Toby Melville) http://rt.com/op-edge/uk-us-special-relationship-690/; President Obama and Prime Minister David Cameron retrieved from International Business Times http://d.ibtimes.co.uk/en/full/247686/obama-cameron.jpg

INTRODUCTION

The United States of America and the United Kingdom of Great Britain and Northern Ireland share close ties diplomatically, culturally, and historically. The two nations have, particularly in recent history, worked together to achieve many of their diplomatic goals. This trans-Atlantic partnership has made sense given the common aims both states share.

Keeping in mind the close relationship between the US and the UK, this paper endeavors to advance US-UK relations by advocating various recommendations in regards to international actors with whom both states are involved. First, we will examine how the US and the UK can enhance the United Nations Security Council to make it more efficient in dealing with military interventions at times of humanitarian crises. Then, we will focus on the NATO intervention in Libya to ascertain the best strategy for continuing the organization's role as a vehicle for US and UK foreign policy goals. Finally, we will take a look at the current threat cyber-warfare poses for both states and how they can counter that threat through international diplomacy.

Improving the United Nations Security Council as a Vehicle for British-American Interests

As members of the Security Council, the United States and the United Kingdom are supported in legitimate interventions by international law; Chapter VII of the United Nations Charter declares that the UN has the authority "in the event of a threat to the peace, breach of the peace, or act of aggression, for the imposition of measures, commonly called sanctions, and the use of armed force".[1] In order to maintain strong and favorable international reputations, as well as to fulfill these two countries' moral commitments to the basic rights enumerated in the Universal Declaration of Human Rights, conducting effective humanitarian interventions is a crucial policy goal of both the United States and the United Kingdom.

In pursuit of this goal, the US and UK have two broad, general options with which to achieve intervention. First, they can use the UNSC to approve multilateral intervention, and second, they can take bilateral or multilateral intervention upon themselves outside of the constraints of the UNSC. Typically, the UNSC is the primary method by which international crises are dealt with. However, if the UNSC is to be the primary vehicle for stopping humanitarian crises, it must be reformed in order to achieve a more flexible, efficient council. Thus, we recommend that in order to further their national security interests, the US and the UK:

1) advocate within the UNSC for a more strict enforcement of sanctions levied by the council, and
2) press for reform which allows a more flexible troop mandate on a case-by-case basis during interventions

We will now address the weaknesses of the UNSC, which will make clear why the reforms we recommend are necessary. Next, we will lay out why each reform is within the best interest of both the US and the UK.

Weaknesses of the Security Council

The Security Council faces several structural problems that affect its ability to fairly intervene in some international conflicts. Five members of the council have permanent seats and all permanent members have veto power. The veto power of Russia and China is often opposed to the humanitarian interests of the US, UK, and France; Russia and China typically vote to not intervene in humanitarian crises, thus blocking the U.N. from intervening at all. Further, notions of sovereignty can make international intervention in humanitarian cases less likely**.** Perhaps the most significant obstacle to realizing US interests via the UNSC is the general inability of the UNSC to enforce its resolution.

Since deference to great powers is built into the structure of the Security Council through the P5 veto power, the Security Council cannot do anything that would upset the most powerful countries. Often, this means one or more of the permanent members does not wish to interfere with another state's sovereignty. In fact, the great powers often either use the Security Council as a "vehicle for their influence" or limit its power and rely instead on regional bodies to prevent/end conflicts.[2]

Yet in many cases, those regional bodies are underfunded and the troops ill-equipped. The African Union's Mission to Somalia's (AMISOM) entire budget is less money than the US spends

[1] Pascal Teixeira, "The Security Council at the Dawn of the Twenty-First Century: To what extent is it willing and able to maintain international peace and security?" (Geneva: United Nations Institute for Disarmament Research, 2003), 3-64.

[2] ibid. 1

on its Afghanistan mission in a day and half.[3] Further, this is not at all unusual for African troops; the African troops composing the UN Assistance Mission to Rwanda (UNAMIR) were significantly less equipped than the Belgian troops of the same mission.[4] In Mali, the American government spent only $4 million on security programs because they feared a military coup, though a military coup resulted anyway and the Malian troops are now poorly trained and work with extremely poor equipment.[5] Yet despite having a dearth of resources, these African troops are expected to carry out peacekeeping missions that their Western counterparts do not wish to take. This arrangement is impractical. Troops with fewer resources are typically far less effective than well-equipped Western troops. Therefore, it is often preferable for the UNSC to intervene rather than deferring to a regional organization.

Sanctions

In many cases, the UNSC decides that an issue does not warrant a military intervention, but does require some sort of action. Generally, the UNSC will then choose to levy sanctions on the actor they find to be at fault. Other times, sanctions can be a compromise if some members wish to pursue intervention but others do not want to act as forcefully. In almost every scenario, sanctions serve as a way for member nations to save face while simultaneously putting pressure on the aggressor in question. In a security or humanitarian crisis, sanctions allow members of the UNSC to still claim they have taken action and publicly condemned the violence without the commitment of peacekeeping forces or some other method of military intervention.

Often however, these sanctions lack any kind of enforcement mechanism. Worse yet, on some occasions members of the UNSC itself are accused of flaunting these sanctions, for example, by trading with states placed under an embargo.[6] In order to address this problem, we recommend that the US and the UK regularly push for secondary sanctions, which we will refer to as "trigger sanctions".

A trigger sanction is a sanction that will come into play if an original sanction is flaunted by a security council member. It acts as an enforcement mechanism. Almost universally, these trigger sanctions would be entirely symbolic and would be diplomatic rather than financial in nature. If, for example, China chose to trade with a state which the security council had chosen to embargo, the other members would publicly denounce China's actions. This is just one example of a possible trigger sanction.

On many occasions trigger sanctions will not be politically feasible. However, the purpose of these sanctions is to enhance the accountability of the Security Council. Therefore, if trigger sanctions are not feasible, we recommend that the US and the UK publicly denounce members who flaunt sanctions without the legal force that a trigger sanction would have.

While these courses of action may just seem like finger-pointing and ambassador-shaming, the entire concept of sanctions tends to be more predicated on style than substance. In other words, most sanctions are meant to channel public denunciation rather than actually financially cripple a state (although there are exceptions). With that in mind, trigger sanctions can keep permanent security council members from "having their cake and eating it too". If security council members are willing to put sanctions in place, they must also be prepared to face the public relations consequences if they do not heed those sanctions themselves.

Mandates

Second, we recommend that the United States and the United Kingdom advocate for more flexible and forceful operation mandates to give UN troops more freedom of action on the ground. Too often, mandates are written with strict limits on U.N. troops, especially regarding use of

---

[3] Audie Cornish and Robert Siegel, "Western Money, African Boots: A Formula for Africa's Conflicts" NPR (March 29, 2013). Audio broadcast.

[4] Samantha Power, "Bystanders to Genocide," *The Atlantic Monthly*, 288 (2001) pp. 84-108: 4.

[5] Mark Moyar ,"How Misguided U.S. Aid Contributed to Mali's Coup," *Bloomberg* (March 11, 2012).

[6] Julian Ryall, "Chinese Firms Breaking UN Embargo on North Korea," *The Telegraph* (June 8, 2012).

violence.[7] Soldiers are limited to self-defense, which is confined to direct attack. For example, forces of the UN mission to the Congo could only use force if opponents attempted to force the troops from a position they already held, to disarm the troops, prevent the troops from carrying out orders of commanding officers, or violate UN installations or abduct UN personnel. But this mandate would not allow the troops to protect citizens of the Congo from attack outside UN ground or attempt any preventative measures. Instead, as the Brahimi report, a report on United Nations Peace Operations from the UN itself, has suggested, mandates should be written to "specify an operation's authority to use armed force in its mandates in order to pose a credible deterrent threat against 'would-be spoilers.'"[8] In other words, mandates should be written to allow troops on the ground more use of force.

We propose several guidelines for how the mandates should be written. First, the mandates should better reflect the realities of the field, including the reality of how much force troops might need to use to accomplish their mission. The Brahimi report insists that the Secretary General "should tell the Security Council what is must know, not what it wants to hear,"[9] yet The assessment of operation by the Security Council is often "insufficient, incomplete or partial", so the mandate writers do not realize how much power the soldiers will need to complete their mission. This presents serious problems for soldiers on the ground. If there is no open conflict, the fact that international peace and security "are threatened or may be threatened is open to challenge;"[10] in other words, soldiers who use violence outside the strict limits of the mandate will not be legally protected for their actions. Instead, mandates should be written to better protect UN troops' right to enforce their mission even if they are not directly attacked.

In order to more effectively write accurate mandates, the Security Council should write the mandates in conjunction with troop-contributing countries and experts on the region in which the UN is intervening. Currently, the Security Council and troop-contributing countries sometimes have different view of objectives of operation and how to achieve them; in fact, the Security Council has been accused of considering troop-contributing countries "mere service providers." However, the Security Council rarely has more extensive knowledge than the countries in which they are intervening, and, in fact, they often have less. For example, when the Security Council oversaw the Bosnia and Kosovo conflicts, the regional reports contained little of substance and were not even read by the Security Council.[11] Instead, the Security Council should gather information from experts and troop-contributing countries when writing mandates. Troop-contributing countries could tailor the mandate to their current strategies and capabilities, and experts could provide the practical details necessary to decide how much force troops might need to use.

Further, the Rules of Engagement can often far too vague, causing difficulties among field commanders who have differences in views of what the Rules of Engagement entail.[12] Mandates written with input from troop-contributing countries will be include better protection for soldiers' actions on the ground, and this wider mandate will lessen friction between commanders in the field. Further, mandates designating clearer authority to use violence to troops will allow troops to better complete their mission, since their actions will not be constrained by fear of legal misinterpretations.

Of course, a mandate allowing broader powers to troops must have some apparatus for monitoring the use of violence. However, the current burden of proof is on soldiers to prove their innocence of wrongful action, and this must be changed. Mandates should provide soldiers with the benefit of the doubt regarding their missions, so that they are better able to respond to changing

---

[7] Hitoshi Nasu, "Enforcement Of Peacekeeping Measures," *International Law on Peacekeeping: A Study of Article 40 of the UN Charter* (Martinus Nijhoff Publishers, 2009), 176-190. Martinus Nijhoff Online. Accessed 5 November 2013.

[8] ibid. 31

[9] United Nations. *Report on the Panel of United Nations Peace Operations*. New York, NY 2000.

[10] ibid. 35

[11] Teixeira, "The Security Council at the Dawn of the Twenty-First Century," 3-64.

[12] Hitoshi, "Enforcement," 190.

circumstances and accomplish their mission.

Conclusion

In conclusion, we make three recommendations for the U.S. and U.K. in regards to humanitarian intervention: bilateral intervention in cases of immediate terrorist threat, rewriting U.N. mandates to include more use of force, and using the U.N. to apply secondary sanctions to countries that do not respect first sanctions. These policies will build up the potential power of the Security Council and the UN, and since the U.N. could be a strong ally in issues of humanitarian crisis and other international conflicts, it is in the interest of the U.S. and U.K. to do so. However, while these reforms will make the UNSC more efficient in handling crises, they do not detract from the power of any of the sovereign members, since our recommendations are carefully predicated on being applied in a case-by-case basis. Further, developing the conflict-resolving capabilities of the UN will add to the reputations of the U.S. and U.K. as strong nations with the power and foresight to support international law and universal justice. Perhaps once these changes are made, further reformation of the U.N. will follow, and future humanitarian crises will be more effectively stopped.

Bibliography

Cornish, Audie and Robert Siegel. "Western Money, African Boots: A Formula for Africa's Conflicts" NPR (March 29, 2013). Audio broadcast.

Nasu, Hitoshi. "Enforcement Of Peacekeeping Measures," *International Law on Peacekeeping: A Study of Article 40 of the UN Charter* (Martinus Nijhoff Publishers, 2009).

Moyar, Mark. "How Misguided U.S. Aid Contributed to Mali's Coup," *Bloomberg* (March 11, 2012).

Power, Samantha. "Bystanders to Genocide," *The Atlantic Monthly*, 288 (2001).

Ryall, Julian. "Chinese Firms Breaking UN Embargo on North Korea," *The Telegraph* (June 8, 2012).

Teixeira, Pascal. "The Security Council at the Dawn of the Twenty-First Century: To what extent is it willing and able to maintain international peace and security?" *Geneva: United Nations Institute for Disarmament Research, 2003*.

United Nations. *Report on the Panel of United Nations Peace Operations*. New York, NY 2000.

The Libyan Intervention and Its Implications for NATO

The US and the UK are both founding members of the North-Atlantic Treaty Alliance (NATO), which acts as a key vehicle in advancing joint foreign-policy goals. In this segment, we will analyze NATO's recent intervention in Libya to determine how the US and the UK can best utilize the organization moving forward. We will advocate for a more centralized command structure within NATO, to better facilitate interventions in the future. NATO would also do well to more clearly delineate the purpose of future interventions, since doing so could accord those actions more legitimacy.

Initially created to protect Western Europe from the German military during the Second World War, NATO shifted its focus to preventing the expansion of the Soviet Union and communism. Upon the collapse of the USSR, NATO was left in a state of flux, since it lacked a central mission. The organization has expanded its mission to provide for the collective defense of all member states. This broader initiative has opened the door for military interventions in regions previously considered to be outside of the reach of NATO, such as Afghanistan and now Libya.

The intervention began in response to the Libyan Civil War, which began in February of 2011. After reports surfaced that Colonel Muammar Gaddafi had conducted airstrikes against Libyan rebels, states began to call for a no-fly zone to be established in Libya. The United Nations then passed UN Security Council Resolution 1973 on 17 March 2011, calling for a no-fly zone, which NATO was meant to enforce. The intervention came to a conclusion upon the death of Colonel Gaddafi.

We will now analyze some of the problems that arose in the Libyan intervention and will then consider what this means for NATO going forward.

Problems within the Libyan intervention

The problems faced by NATO in the intervention can be broadly grouped into three categories: mission creep, an imbalance of contributions, and inefficient central command.

Contrasting its initial intention with the final result, it is clear that the intervention suffered from mission creep, an unintentional expansion of the boundaries of a military engagement. The justification for military intervention in Libya was United Nations Security Council Resolution 1973.[13] At the beginning of March of 2011, NATO agreed to launch an operation to enforce the arms embargo against the country. Then it agreed to enforce the UN-mandated no-fly zone over Libya. By the end of March the intervention's three focuses were the arms embargo, the no-fly zone, and strikes on military forces that were threats to civilians.[14]

Initially, changing the regime in Libya was not the focus of the intervention.[15] Through protecting civilians, the coalition became involved in regime change, because they had to stop the Libyan army from attacking the rebels or getting near the rebels' stronghold. As a result, NATO took on a more offensive role, striking military targets of the Libyan military. While this changed the result and goal of the mission, it was still conducted with the justification that it was necessary to protect civilians.[16] It is evident that the nature of NATO's involvement with the conflict changed over time but not in a way that reflected the original UN resolution. This mission creep harms the legitimacy of NATO interventions, since it gives the appearance of untrustworthiness. Public opinion

---

[13] United Nations, "Security Council Approves 'No-Fly Zone' over Libya, Authorizing 'All Necessary Measures' to Protect Civilians, by Vote of 10 in Favour with 5 Abstentions." *UN News Center*. 17 Mar 2011.
[14] North Atlantic Treaty Organization, "NATO and Libya." 28 Mar 2012.
[15] Jason Cook, "Libya's Lessons on Syria." Foreign Policy.
[16] Ibid.

and the opinion of non-member states of NATO will be less favorable if these groups are convinced that NATO will expand beyond its initial role in a military engagement.

Additionally troubling was the imbalance of contributions made by member-states to the intervention. The imbalance of military spending by NATO's member nations represents a serious problem regarding NATO's effectiveness as a tool to ease the logistical burden of expeditionary operations. Because most of NATO's member states have underinvested in their respective militaries, with European spending falling from 34% of the alliance total in 1991 to 21% today, many of NATO's member states lack the key logistical capabilities that a successful intervention entails.[17] In the case of Libya, the United States needed to provide a substantial quantity of hardware and personnel for tasks such as refueling aircraft, information technology, and similarly crucial military functions, because its European partners did not possess the capability to perform these functions on their own. [18] Crucially, the intervening force suffered from a shortage of surveillance equipment and trained target selectors, creating inefficiencies in the machinery of the operation.[19]

As former United States Secretary of Defense, Robert Gates noted, "while every alliance member voted for the Libya mission, less than half have participated, and fewer than a third have been willing to participate in the strike mission."[20] Underfunding prevented many members from participating. In fact, only five of the 28 NATO allies meet NATO's recommendation that countries should spend at least 2% of GDP on defense: the US, the UK, France, Greece and Albania.[21]

The vast majority of military supplies and actions were controlled by the United States, with the UK and France following behind. Of the total strikes done over the course of the intervention, however, France performed 33%, the UK 21%, and the US 19%. The US, the UK, and France also supplied the vast majority of personnel.[22] A similar pattern follows with the provision of aircrafts. Providing these military supplies meant that the United States, the United Kingdom, and France also had the largest financial burden. The US spent approximately $1.1 billion while the UK and France each spent up to $480 million. The only common funds accounted allocated to the Libya mission were those used for NATO's Airborne Warning and Control System.[23] This imbalance is worrisome, as NATO has the potential to strengthen its member states' communication and intelligence gathering capabilities, but only if the proper military infrastructure exists. Because the Libyan intervention was relatively small in scale, these problems did not generate a serious possibility of failure, but in a larger intervention, NATO might find itself under-equipped to adequately carry out its mission.

Furthermore, strategic planning in the Libyan intervention was hurried. The United Nations Resolution 1973 which officially authorized the actions in Libya was passed on March 17, 2011. Military operations started a scant two days later with French and American forces hitting Libyan targets on March 19th. These initial engagements were focused on ensuring the protection of civilians and opposition activist especially around the

---

[17] Anders Fogh Rasmussen, "NATO after Libya: The Atlantic Alliance in Austere Times." *Foreign Affairs.* 90 (2011): 2.
[18] Ivo H. Dadlder and James G. Stavridis, "NATO's Victory in Libya,'." *Foreign Affairs* 91, no. 2 (2012).
[19] Douglas Barrie, "Libya's Lessons: The Air Campaign." *Survival* 54, no. 6 (2012): 57-65.
[20] Donna Miles, "NATO Members Re-evaluate Contributions to Libya." American Forces Press Service, 14 June 2011.
[21] The Economist, "Always Waiting for the US Cavalry." *The Economist*. 10 June 2011.
[22] C.J. Chivers and Eric Schmitt, "In Strikes on Libya by NATO, an Unspoken Civilian Toll." *The New York Times*. 17 Dec 2011.
[23] Miles, "NATO Members Re-evaluate Contributions to Libya."

city of Benghazi.[24] Forces under the NATO mandate officially took over duties such as responsibility for the no-fly zone and arms embargo approximately five days later.

Information also suggests that there was debate within the organization of what the final command and control chain of authority should be, with French, German, and Turkish representatives expressing reservations about the role of the NATO command structure in the operation.[25] Considering the necessary speed with which the coalition and NATO were forced to act by the events on the ground in Libya, it is likely that there was less extensive planning than is ideal beforehand, leading to the fluidity of the operation and uncertainty regarding the correct command and control structure.

In the modern conflicts in which the United States and the United Kingdom engage, particularly interstate conflicts, force effectiveness has become less related to raw quantities of assets and manpower, and more related to fluid command and communication structures.[26] This shift in conflict dynamics has influenced the determinants of effective expeditionary operations, placing a greater emphasis on communication between agencies.[27] This is to say that evolving technology over the last several decades has engendered a "network-centric" operational framework, competing with the traditional "platform-centric" operational framework, shifting focus to a different set of key determinants of effectiveness.[28] Given the necessity for effective networks of communication, an organization such as NATO has a crucial logistical role to play in carrying out effective interventions. That is, NATO can provide a unified command structure that can be mobilized far more quickly than its equivalent in an ad hoc alliance.[29] Further, with the proper organizational machinery in place, NATO has the potential to appreciably diminish the imbalance in costs to its member states in the event of an intervention because the unified command structure allows smaller states to play a larger role than they would in an ad hoc alliance.[30] It is because NATO has such considerable potential to facilitate effective expeditionary operations that the current state of the alliance is so troubling.

Recommendations Going Forward

The aforementioned problems that arose within the Libyan interventions provide unique challenges which NATO must face. The first problem, mission creep, is perhaps the most easily fixed. Given the shifting goal posts that were NATO's aims throughout the intervention, it would behoove the US, the UK, and their NATO partners to more clearly define the goals of an intervention before it begins. While the initial objective was to create a no-fly zone in accordance with the UN resolution, there was too little focus on the outcome that this no-fly zone was meant to produce.

However, defining future missions more clearly does present some challenges, given the structural causes of the problem. As mentioned, NATO has lost its original precise mission and has instead focused on collective security, much like an alliance in the

---

[24] Claire Taylor and Ben Smith, "Military Operations in Libya." House of Commons Library. 1 Apr 2011.
[25] Ibid..
[26] Max Boot, "The new American way of war." *Foreign Affairs* (2003): 41-58.
[27] Robert C. Egnell, "Explaining US and British performance in complex expeditionary operations: The civil-military dimension." *The journal of strategic studies* 29, no. 6 (2006): 1041-1075.
[28] John R. Lindsay, "Reinventing the Revolution: Technological Visions, Counterinsurgent Criticism, and the Rise of Special Operations." *Journal of Strategic Studies* ahead-of-print (2013): 1-32.
[29] Dadlder and Stavridis, "NATO's Victory in Libya,'." *Foreign Affairs* 91, no. 2 (2012).
[30] Ibid.

traditional sense of the term. A refocusing of the organization's broader mission could help clarify the objectives of specific interventions, making mission creep a less likely phenomenon. For instance, while justification for the Libyan intervention cited the Right to Protect doctrine, which advocates for the protection of people under attack from their own government, it is unclear how protecting the Libyan people advanced the collective security of NATO. If NATO wishes to continue a more global approach, intervening in conflicts not directly involving member-states, it would be best to redefine the organization's broader mission to include said approach. Otherwise, there are no limitations to the role of NATO in international conflicts.

Second, the imbalance in funding and participation defines NATO as a lopsided organization. However, this imbalance is completely unlikely to end. That said, this imbalance, when combined with the hurried methods of the Libyan intervention, created a confused central command structure and harmed the ability of NATO forces to communicate effectively. While smaller NATO members will not suddenly shift all of their expenditures into military technology, steps can be taken to increase the efficiency of NATO when it chooses to intervene abroad.

While the broader command structure of NATO's military forces is sensible, the issue arises when interventions actually occur. Each intervention includes a different ad-hoc alliance of members within NATO since, as was mentioned earlier, many nations choose not to participate. The different combinations of states create tension and confusion as to who is in control. Thus, to aid NATO central command, future interventions should create a panel with representatives from each participating country, so that faster decision-making can occur between those who have something on the line.

The Libyan intervention ended well from most perspectives. That said, it was not perfect. If NATO takes our recommendations into account, we believe that it could become a more effective vehicle for advancing its members' interests, particularly in the case of the US and the UK.

Bibliography

Bajoria, Jayshree, and Robert McMahon. "The Dilemma of Humanitarian Intervention." Council on Foreign Relations. http://www.cfr.org/humanitarian-intervention/dilemma-humanitarian-intervention/p16524.

Baraki, Spencer. "The New Humanitarian Precedent: Bosnia, Kosova, and the Libyan Intervention of 2011." The University of Alberta. http://ejournals.library.ualberta.ca/index.php/eudaimons/article/download/11879/9038.

Barrie, Douglas. "Libya's Lessons: The Air Campaign." *Survival* 54, no. 6 (2012): 57-65.

Boot, Max. "The new American way of war." Foreign Affairs (2003): 41-58.

Brunnstrom, David, and Adrian Croft. "Analysis: Looming end of Afghan mission leaves NATO with identity crisis." Reuters. http://www.reuters.com/article/2012/05/23/us-nato-summit-future-idUSBRE84M02E20120523 (accessed December 8, 2013).

Chivers, C.J. and Eric Schmitt. "In Strikes on Libya by NATO, an Unspoken Civilian Toll." The New York Times. 17 Dec 2011. http://www.nytimes.com/2011/12/18/world/africa/scores-of-unintended-casualties-in-nato-war-in-libya.html?pagewanted=all&_r=0

Chivvis, Christopher S. "Libya and the Future of Liberal Intervention." *Survival*54, no. 6 (2012): 69-92.

Dadlder, Ivo H., and James G. Stavridis. "NATO's Victory in Libya,'." *Foreign Affairs* 91, no. 2 (2012).

The Economist, "Always Waiting for the US Cavalry." *The Economist.* 10 June 2011. http://www.economist.com/blogs/charlemagne/2011/06/libya-europe-and-future-nato/print

Egnell, Robert C. "Explaining US and British performance in complex expeditionary operations: The civil-military dimension." The Journal of Strategic Studies 29, no. 6 (2006): 1041-1075.

Flamini, Ronald. "Future of NATO." CQ Researcher by CQ Press. http://library.cqpress.com/cqresearcher/document.php?id=cqrglobal2009010000&type=hitlist&num=0#.UoGBlZTwJwp.

Lindsay, John R. "Reinventing the Revolution: Technological Visions, Counterinsurgent Criticism, and the Rise of Special Operations." Journal of Strategic Studies ahead-of-print (2013): 1-32.

Lynch, Marc. "What the Libya Intervention Acheived." Foreign Policy. http://lynch.foreignpolicy.com/posts/2011/10/27/what_the_libya_intervention_achieved .

Mezran, Karim, Jason Pack, and Haley Cook. "Libya's Lessons On Syria - By Karim Mezran, Jason Pack, and Haley Cook | The Middle East Channel." Foreign Policy. http://mideast.foreignpolicy.com/posts/2013/09/04/libyas_lessons_on_syria.

Miles, Donna. "NATO Members Re-evaluate Contributions to Libya." American Forces Press Service, 14 June 2011. http://www.defense.gov/News/NewsArticle.aspx?ID=64305.

North Atlantic Treaty Organization, "NATO and Libya." NATO, 28 Mar 2012. http://www.nato.int/cps/ar/natolive/topics_71652.htm .

Nyiri, Zsolt, and Joshua Raisher . "GMF - The German Marshall Fund of the United States - Strengthening Transatlantic Cooperation." German Marshall Fund of the United States. http://www.gmfus.org/archives/transatlantic-trends-public-opinion-and-nato/.

Pack, Jason, Haley Cook, and Kalim Mezran. "Libya's Lessons on Syria." Foreign Policy. http://mideast.foreignpolicy.com/posts/2013/09/04/libyas_lessons_on_syria.

Rasmussen, Anders Fogh. "NATO after Libya: The Atlantic Alliance in Austere Times." *Foreign Aff.* 90 (2011): 2.

"Security Council Approves 'No-Fly Zone' over Libya, Authorizing 'All Necessary Measures' to Protect Civilians, by Vote of 10 in Favour with 5 Abstentions." *UN News Center*. UN, 17 Mar 2011. http://www.un.org/News/Press/docs/2011/sc10200.doc.htm.

Shanker, Thom. "Defense Secretary Warns NATO of 'Dim' Future - NYTimes.com." New York Times. http://www.nytimes.com/2011/06/11/world/europe/11gates.html?_r=1&.

Taylor, Claire and Ben Smith. "Military Operations in Libya." House of Commons Library. 1 Apr 2011. http://www.parliament.uk/briefing-papers/SN05909.pdf.

United Nations. "Security Council Approves 'No-Fly Zone' over Libya, Authorizing 'All Necessary Measures' to Protect Civilians, by Vote of 10 in Favour with 5 Abstentions." UN News Center. http://www.un.org/News/Press/docs/2011/sc10200.doc.htm.

Cyber Security: A New Frontier of National Security

An increased reliance on computers in all facets of governance, while enhancing security in some ways, has increased vulnerability in others. Technology has amplified the ability of various groups, both state actors and non-state actors, to cause disruptions in the national security of others. In this section, we will examine the challenges presented by the growing manifestation of cyber warfare and will then offer recommendations that both the US and the UK can undertake to improve cyber security.

Russia

The ongoing threats to cyber security from Russia is an issue of critical importance for United States and the United Kingdom, as well as for the international community as a whole. Steps have been taken to curtail the consequences of cyber warfare but have thus far proven to be largely ineffective. While security breaches are the primary concerns, the plausibility and extent of control over the web and the cyber world must also be investigated before adopting policy changes. Furthermore, previous attacks attributed to Russia and the damage they have caused need to be analyzed. This will help us to understand the magnitude of possible threats to the U.S. and the U.K., as well as to minimize our chances of repeating mistakes.

Following tensions left from the Cold War, there have been attempts to strengthen relations between both countries with the signing of the new START Treaty, reducing the amount of nuclear weapons in their possession, and with the creation of the Bilateral Presidential Commission. Yet, as the Brookings Institute informs, tensions continue to exist as there are disagreements over missile defense in Europe, the future of Syria, and human rights in Russia.[31] In short, while there have been greater moves toward better relations, there are still existing tensions and a continuation of mutual deterrence. In 2013, the U.S. and Russia signed an agreement to create a communication link on cyber security to prevent conflict.[32]

The relations between Russia and the U.K. "have been damaged by a number of problems."[33] These problems include human rights violations, Syria, and the closing of British Council offices in Russia by the Russian government.[34] Their relationship has been further damaged with the revealing of espionage conducted on the U.K. by Russia in attempts to gain information on Russian oligarchs and access to secrets of the U.S. government.[35] Yet, the U.K. has also been responsible for conducting espionage on Russia and has publicly admitted to such activities.[36]

Russia is a threat to the cyber security of the U.S. and the U.K. not only because of existing tensions and distrust, but also because of their cyber capabilities and international cyber attacks in the past. Russia has been suspected of leading cyber-attacks against

---

[31] Steven Pifer, "The Future Course of the U.S.-Russia Relationship."

[32] Ellen Nakashima, "U.S. and Russia sign pact to create communication link on cyber security," *The Washington Post*.

[33] Ben Smith, "UK relations with Russia." October 25, 2012.

[34] Ibid.

[35] Ibid.

[36] "UK Spied on Russians with Fake Rock," *BBC,* edited January 18, 2012.

Estonia and Georgia.[37] The Russian government has the capacity to create "long-term, wide-scale disruption of services, such as regional power outages" because they have the "level of technical expertise and operational sophistication required for such attack—including the ability to create physical damage or overcome mitigation factors like manual overrides." Without threats from or conflict with the U.S., attacks from Russia are unlikely, but there is a more serious threat from other motivated actors within Russian that are not associated with the central government. Even "unsophisticated" attacks could target "poorly protected U.S. networks that control core functions, such as power generation."[38]

Taking into consideration previous cyber-attacks that Russia has been accused of committing against Estonia and Georgia, existing threats from Russia and the growing cyber world, both the United States and the United Kingdom must more comprehensively address the issue of cyber security and cyber threats. Both countries must increase their bilateral cooperative efforts with Russia. Our proposal has two goals: decreased tensions between Russia and the U.S. and the U.K. which pose severe threats to cyber security and increased transparency in cyber capabilities and actions. The United States and Russia have demonstrated interest in creating a bridge of communication to prevent misunderstandings over national security in the cyber world through the creation of a "hotline" between the U.S. Cyber Security Coordinator and the Russian Deputy Secretary of the Security Council.[39] It must be recognized that there are conflicts in the capacity of such organizations to regulate cyberspace and to prosecute cyber-attackers because of the complexities of determining culpability in the cyber world; yet, steps can be taken to secure the clarity surrounding each countries cyber activities.

We propose to facilitate cooperation through the creation of a forum that develops transparency on the actions and intentions of the U.S., the U.K., and Russia in the cyber world. Building on the existing communication and discussions over threats and use of Information and Communication Technologies,[40] a conversation can be initiated to develop a framework of cyber-laws that benefits both nations. This forum would also include a neutral nation as a mediator and could potentially become an example for dealing with cyber security issues with other countries.

China

Cyber security issues pose unique challenges to U.S.-China relations. Understanding the challenges presented requires adequately distinguishing among the challenges presented, ranging from cyber-espionage to cybercrime. While the former has become, as revelations by Edward Snowden clearly demonstrate, quite pervasive throughout intelligence communities worldwide, the latter has inflicted primarily economic costs on businesses. General Keith Alexander, head of the National Security Agency and U.S. Cyber Command, calls intellectual property theft via cyber espionage "the greatest transfer of wealth in human history," estimating the costs to the U.S. at approximately

---

[37] Major William C. Ashmore, "Impact of Alleged Russian Cyber Attacks."

[38] Office of the Director of National Intelligence. Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence.

[39] The White House, Office of the Press Secretary. FACT SHEET: U.S.-Russia Cooperation on Information and Communication Technology Security.

[40] The White House, Office of the Press Secretary. Joint Statement on the Inaugural Meeting of the U.S.-Russian Bilateral Presidential Commission Working Group on Threat to and in the Use of Information and Communication Technologies (ICTs) in the Context of International Security.

$340 billion annually.[41] While the alleged theft of U.S. intellectual property by Chinese entities has frequently been a source of friction, the central national security issues at stake are beyond these economic costs to U.S. businesses. Notably, the "Comment Crew," Shanghai-based hackers working out of a PLA-owned building conducted a sustained campaign against more than twenty foreign defense contractors, seeking to acquire the technology underlying the U.S. superiority in the development of military drones.[42] This campaign corresponded closely with ambitious efforts by the Chinese government and People's Liberation Army to accelerate the development of China's drone program. According a 2012 report by the Defense Science Board, a Pentagon advisory committee, "The military significance of China's move into unmanned systems is alarming." In this and other cases, the Chinese government has sought to maintain a degree of plausible deniability; attribution of specific attacks or operations to state-sponsored rather than non-state actors remains a challenge and introduces a further source of ambiguity. Indeed, the cyber domain has posed new and unanticipated national security challenges, the implications of which policymakers may not be yet prepared to consider.

Looking to the future, the truly serious threats to the stability of the cyber domain lie in the increasing tendency towards the development of offensive capabilities. Scenarios of cyber war envision attacks on critical infrastructure that cross the boundary between cyber and kinetic warfare, scenarios that have seemed increasingly plausible since the U.S. deployment of Stuxnet against Iran. Certain ambiguities persist in the characterization of "cyberattacks" and "cyberwar," but, by Joseph Nye's definition, cyberwar entails "any hostile action in cyberspace that amplifies or is equivalent to major physical violence."[43] The Obama administration has moved to establish "Offensive Cyber Effects Operations," which "can offer unique and unconventional capabilities to advance US national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging."[44] This has entailed developing a list of overseas targets for U.S. cyberattacks, raising concerns about the militarization of the Internet. So too, the PLA has developed a framework of "information confrontation," adopting a strategy of "Integrated Network Electronic Warfare" with a focus on enhancing the coordination of offensive and defensive cyber-missions and centralized command authority. That PLA analysts point to U.S. logistics and Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) infrastructure as "strategic centers of gravity" suggests that the PLA would seek to target these systems prior to a combat scenario.[45] In this regard, with concerns over the potential for such preemption, the cyber domain presents a prevailing source of insecurity that may intensify mutual distrust and intensify the preexisting security dilemma in U.S.-China relations.

The fundamental question facing policy makers and academics alike is the extent to which conventional paradigms of international relations apply in cyberspace. Here, as in the case of terrorism, the prevalence and power of individual non-state actors introduces a

---

[41] Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History,'" The Cable blog on ForeignPolicy.com, July 9, 2012.

[42] Wong, Edward, "Hacking U.S. Secrets, China Pushes for Drones," *New York Times*, September 20, 2013.

[43] Nye, Joseph S., "The Mouse Click That Roared," *The Korea Times, September 13, 2013*

[44] Greenwald, Glenn and Ewen MacAskill, "Obama orders US to draw up overseas target list for cyber-attacks," *The Guardian*, June 7, 2013.

[45] Brian Krekel, Patton Adams and George Bakos. "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Northrop Grumman Corp. 7 Mar 2012.

major element of uncertainty, yet deterrence dynamics are likely to be equally viable in the cyber domain.[46] Sophisticated and resilient cyber security measures are critical in the defense of key assets and infrastructure, while also discouraging would-be attackers. So too, what has been termed Active Cyber Defense (ACD), which, unlike "passive" defenses that merely seek to prevent intrusion, entails "proactive actions that engage the adversary before and during a cyber incident," such as retaliatory hacking, offers an alternative for policymakers.[47] Yet the U.S. must not go too far. The consideration of a strategy of nuclear deterrence in cyberspace introduces an unnecessarily dangerous dynamic and could exacerbate preexisting instabilities in U.S.-China relations.[48]

On the other hand, the emergence of institutionalized mechanisms for bilateral dialogue on cybersecurity issues is a positive trend and should be sustained. In June 2013, the U.S. and China discussed these "thorny" issues during the China-U.S. Strategic and Economic Dialogue (S&ED), on issues including establishing a bilateral cyber working group, developing international cyberspace rules, and implementing additional measures to boost dialogue and cooperation on cyber security.[49] It is essential to expand and regularize such dialogues and exchanges, while seeking to promote cooperation in areas in which there is a possibility of consensus, such as cybercrime, which is illegal within most jurisdictions. So too, the development of an international regime or international norms on cyberspace represents an area in which the U.S. and China might be able to establish basic ground rules and understandings of each other's "red lines."

Terrorist Organizations

In September 2012, several major banks including J.P. Morgan and Chase, Bank of America, Wells Fargo, U.S. Bank, and PNC bank were attacked and their websites were shut down. Izz ad-Din al-Qassam Cyber Fighters, a military branch of Hamas, called the attack "Operation Ababil." They claimed responsibility for the attacks, and at the time they claimed they were in response to the "Innocence of Muslims" video that caused controversy and protests in 2012. Their action was a Denial of Service (DoS) attack which caused bank websites to shut down but did not compromise financial information[50]. However, the attack was better coordinated than any previous terrorist cyber attack, and CNN called the attacks "the biggest cyber attacks in history"[51].

At the moment, the consensus by the FBI and NSA is that terrorist groups do not have the technological sophistication to launch a large scale cyber attack, but they are taking a series of measures to prepare.

There is growing concern of terrorist groups increasing their ability to use cyber attacks in response to the improved international physical and border security and the published computer security weaknesses of the United States.[52] In March of 2012, FBI Director Robert Mueller expressed concern that terror groups are becoming more cyber savvy. Al-Qaeda recently began to publish an online magazine called "Inspire," and a

---

[46] Nye, Joseph S., "The Mouse Click That Roared," *The Korea Times, September 13, 2013*

[47] Lachow, Irving, "Active Cyber Defense: A Framework for Policymakers," Center for a New American Security, February 2013.

[48] Farnsworth, Timothy, "Is There A Place For Nuclear Deterrence in Cyberspace?" May 30, 2013.

[49] "China, U.S. discuss cyber security," Xinhua, July 9, 2013.

[50] Paul Rothman, "Cyber terror rages in the banking sector," *Securityinfowatch.com*, September 28, 2012.

[51] David Goldman, "Major Banks hit with the biggest cyberattacks in history," *CNNMoney*. September 28, 2012

[52] "Terrorist Capabilities for Cyberattack: Overview and Policy Issues," *CRS Report for Congress*, January 22, 2007.

Somali group Al-Shabaab uses its Twitter account to publicize and organize. The general increase in terror groups' use of cyberspace to organize and conduct their business could lead to more successful online attacks.[53]

There are several issues which must be addressed to prevent future cyber attacks. There should be increased cooperation between private companies and the federal government, both of which have come under attack by various cyber forces.[54] Increasing collaboration between the government and its corporations would lower the effectiveness of cyber-attacks. The second issue is the extent to which counterterrorism efforts are linked with international cybercrime prevention efforts.[55] The collaboration and increase of information-sharing between organizations in both fields will help identify and prevent cybercrime and cyber criminals.

Some steps have already been taken to protect against cyber-attacks. In 2007, the Congress passed a law that allows the Department of National Security Secretary to assess grants for national security based on their ability to prevent cyber threats. In 2012, Congress passed the Cybersecurity Act, which gives the Department of Homeland Security more influence in the development and testing of cyber initiatives and allowed the National Information Sharing Organization to guide an increase in cooperation between federal agencies.[56]

In March 2013, the Pentagon established 13 "cyber teams" to combat cyber attacks. General Keith Alexander's reporting of this addition to the Senate Armed Services Committee was the first definitive government official statement that the U.S. is deploying cyber weapons.[57]

Paths forward should be oriented towards establishing revisions in the collaborative frameworks of government agencies, rather than legislative change, which could be significantly harder to materialize in the near future.

In order to acquire more effective means of combating small-scale cyber-attacks, the US and U.K. should pursue channels for disseminating information between corporations and federal institutions. More specifically, these channels should be designed to facilitate communication about potential threats between federal institutions specializing in national security and technology and large-scale companies that face cyber-attacks.

Second, the US and the UK should bridge counterterrorist organizations with international cybercrime prevention efforts as a means of consolidating information. By creating sustained channels of information sharing on the cyber efforts of terrorist groups and the cyber efforts of criminal groups, both the US and the UK will enjoy greater cyber security.

---

[53] Luis Martinez, "Intel Heads Now Fear Cyber Attack More Than Terror," ABC News, 13 March 2013.

[54] John Rollins and Clay Wilson, "Terrorist Capabilities for Cyberattack: Overview and Policy Issues," *Congressional Research Service/The Library of Congress*, January 22, 2007.

[55] Ibid.

[56] Martinez, "Intel Heads Now Fear Cyber Attack More Than Terror."

[57] Ibid.

Bibliography

British Broadcasting Corporation. “UK Spied on Russians with Fake Rock,” BBC, 18 Jan 2012,http://www.bbc.co.uk/news/world-europe-16614209. “China, U.S. discuss cyber security,” Xinhua, July 9, 2013.

Farnsworth, Timothy. “Is There A Place For Nuclear Deterrence in Cyberspace?” May 30, 2013.

Goldman, David. “Major Banks hit with the biggest cyberattacks in history,” *CNNMoney*. September 28, 2012.

Greenwald, Glenn and Ewen MacAskill. “Obama orders US to draw up overseas target list for cyber-attacks,” *The Guardian*, 7 June 2013, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

Krekel, Brian, Patton Adams and George Bakos. "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Northrop Grumman Corp, 7 Mar 2012, http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_ Capabilities_for _Computer_Network_Operations_and_Cyber_%20Espionage.pdf.

Lachow, Irving. “Active Cyber Defense: A Framework for Policymakers,” Center for a New American Security, February 2013, http://www.cnas.org/sites/default/files/publications pdf/CNAS_ActiveCyberDefense_Lachow_0.pdf.

Martinez, Luis. "Intel Heads Now Fear Cyber Attack More Than Terror," ABC News, 13 March 2013, http://abcnews.go.com/Blotter/intel-heads-now-fear-cyber-attack-terror/story?id=18719593.

Nakashima, Ellen. “U.S. and Russia sign pact to create communication link on cyber security,” *The Washington Post*. http://articles.washingtonpost.com/2013-06-17/world/40025979_1_cyber-security-pact-homeland- security.

Nye, Joseph S. “The Mouse Click That Roared,” *The Korea Times*, September 13, 2013.

Office of the Director of National Intelligence. "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community." Senate Select Committee on Intelligence. http://www.intelligence.senate.gov/130312/clapper.pdf.

Pifer, Steven. “The Future Course of the U.S.-Russia Relationship.” The Brookings Institution, 21 Mar 2012, http://www.brookings.edu/research/testimony/2012/03/21-arms-control-pifer.

Rogin, Josh. “NSA Chief: Cybercrime Constitutes the ‘Greatest Transfer of Wealth in History,’” *Foreign Policy*, 9 July 2012, http:// thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_ constitutes_the_greatest_transfer_of_wealth_in_history.

Rollins, John and Clay Wilson. “Terrorist Capabilities for Cyberattack: Overview and Policy Issues,” *Congressional Research Service/The Library of Congress*, January 22, 2007, http://www.fas.org/sgp/crs/terror/RL33123.pdf.

Rothman, Paul. “Cyber terror rages in the banking sector,” *Securityinfowatch.com*, September 28, 2012, http://www.securityinfowatch.com/blog/10796084/cyber-terror-rages-in-the-banking-sector.

Smith, Ben. “UK relations with Russia.” House of Commons, 25 Oct 2012, http://www.parliament.uk/briefing- papers/SN06449.

“Terrorist Capabilities for Cyberattack: Overview and Policy Issues,” *CRS Report for Congress*, January 22, 2007, http://www.fas.org/sgp/crs/terror/RL33123.pdf.

The White House, Office of the Press Secretary. "FACT SHEET: U.S.-Russia Cooperation on Information and Communication Technology Security." http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.

The White House, Office of the Press Secretary. "Joint Statement on the Inaugural Meeting of the U.S.-Russian Bilateral Presidential Commission Working Group on Threat to and in the Use of Information and Communication Technologies (ICTs) in the Context of International Security." http://www.whitehouse.gov/the-press-office/2013/11/22/joint-statement-inaugural-meeting-us-russia-bilateral-presidential-commi.

Wong, Edward, “Hacking U.S. Secrets, China Pushes for Drones,” *New York Times*, 20 September 2013, http://www.nytimes.com/2013/09/21/world/asia/hacking-us-secrets-china-pushes-for-drones.html