The history of international cybersecurity politics essay

The United States, England, and Continental Europe have very different approaches to cybersecurity. The United States and United Kingdom conceive of cyber primarily as a national security problem to be handled by the military- which in turn sees the Internet as a fifth domain of war to be dominated. The rest of the European Union, however, sees cyber threats mostly as an irritant for commerce and individual privacy that should be dealt with by civilian authorities working in combination with private enterprise.

Additionally, while the United States can have a single policy, even though its one implemented by many different federal departments, the European Union is made up of twenty-seven nations with their own laws, notions, and philosophical differences over how to approach cyber issues. Finally, there is NATO, where a unified transatlantic cyber vision must be reconciled and arranged in a coherent manner among twenty-eight allies through a cumbersome bureaucratic process. To make sense of these conflicting visions, this essay reviews cyber attacks against NATO members, attempts to outline the challenges of developing a transatlantic vision for cyber policy, and highlights some of the fundamental differences among NATO members.

It is helpful to remember that although the Internet is so ensconced in most of our lives that it is hard to envision living without it, the first modern Web browser didn’t debut until 1993 and broadband access has only become widespread over the last decade. As a result, senior government and military leaders did not grow up with the Internet and are gradually having to adapt to emerging cyber realities. Franklin Kramer, who worked as assistant secretary of defense under President Bill Clinton, draws a comparison with

the Great Fire of London, he notes that it nearly destroyed the city in 1666 “ because an advance in living conditions- wooden houses for many- was not matched by security measures. There were no firefighting technologies, no firefighting processes, and no resources devoted to fire fighting.” This was still true more than two centuries later with the Great Chicago Fire. Despite our slow learning curve, “ in the modern world, while fire may strike, it is not the city-devouring scourge that it once was.” Through government regulations that established building codes and through volunteer and government-run fire departments, a protective-response was established over the centuries.[1]

Former Deputy Secretary of Defense William J. Lynn III uses a more aggressive analogy: “ The first military aircraft was bought, I think, in 1908, somewhere around there. So we’re in about 1928,” he said. “ We’ve kind of seen some … biplanes shoot at each other over France,” he added. “ But we haven’t really seen kind of what a true cyberconflict is going to look like.”[2]

Currently, European policymakers seem to treat cybersecurity more along fire-prevention lines rather than as biplanes over France. And framing is critical when thinking about cyber issues. As Kramer observes, “ Ask the wrong question, and you generally will get the wrong answer. And cyber- and what to do about cyber conflict- is an arena where there is generally no agreement on what is the question, certainly no agreement on what are the answers, and evolving so fast that questions are transmuted and affect and change the validity of answers that have been given.” He argues that the lack of agreement over the nature of the problem, lack of coherent regulation and authority mechanisms, and conflict between connectivity and

security together make cyber a “ wicked problem” not easily susceptible to resolution.[3]

Lynn manages to frame the issue in military and security terms but fully acknowledges that the reality is quite blurred and that no clear lines exist in this new domain. “ I mean, clearly if you take down significant portions of our economy we would probably consider that an attack. But an intrusion stealing data, on the other hand, probably isn’t an attack. And there are [an] enormous number of steps in between those two.”[4]

Lynn goes on to say, one of the challenges facing Pentagon strategists is “ deciding at what threshold do you consider something an attack... I think the policy community both inside and outside the government is wrestling with that, and I don’t think we’ve wrestled it to the ground yet.” In other words, it is difficult to know whether the house is on fire or biplanes are shooting at each other.[5]

Correspondingly tricky, defense officials say, is how to pinpoint who is doing the attacking. This raises further complications that are clearly at the heart of the Pentagon’s mission. At the Council on Foreign Relations Lynn summarized the issue “ If you don’t know who to attribute an attack to, you can’t retaliate against that attack,” As a result, “ you can’t deter through punishment, you can’t deter by retaliating against the attack.” He discussed the complexities that make cyberwar so different from, say, “ nuclear missiles, which of course come with a return address.”[6]

The cyber threat is very much a part of our current reality. Over the last several years several NATO members and partners, including the United States, have been targeted by severe cyber attacks.

Estonia

What is commonly believed to be the “ first known case of one state targeting another by cyber-warfare” began on April 27, 2007, when a massive denial-of-service attack was launched by Russia against Estonia over a dispute involving a statue. The attack crippled “ websites of government ministries, political parties, newspapers, banks, and companies.”[7]The attack was nicknamed Web War One and it caused a resonation within transatlantic national security circles.[8]

The German newspaper Deutsche Welle wrote that “ Estonia is particularly vulnerable to cyber attacks because it is one of the most wired countries in the world. Nearly everyone in Estonia conducts banking and other daily activities on line. So when the cyber attack occurred, it nearly shut Estonia down.”[9]Then-EU Information Society and Media commissioner Viviane Reding called the attacks “ a wakeup call,” commenting that “ if people do not understand the urgency now, they never will.” Her reaction was to incorporate a response into an EU-wide law on identity theft over the Internet.[10]Additionally, NATO did establish a Cyber Center of Excellence in Tallinn, which will be discussed later in the essay.

Georgia

While not a NATO member, Georgia is a NATO partner, and the April 2008 Bucharest Summit declared that it “ will become a member” at some

unspecified time in the future, a promise reiterated at the November 2010 Lisbon Summit.[11]Weeks before the August 2008 Russian land invasion and air attack, Georgia was subject to an extensive, coordinated cyber attack. American experts estimated that the “ attacks against Georgia’s Internet infrastructure began as early as July 20, with coordinated barrages of millions of requests- known as distributed denial of service, or DDOS, attacks- that overloaded and effectively shut down Georgian servers.”[12]The pressure was intensified during the early days of the war, effectively shutting down critical communications in Georgia.

After defacing Georgian President Mikheil Saakashvili’s web site and integrating a slideshow portraying Saakashvili as Hitler, coming up with identical images of both Saakashvili and Hitler’s public appearances, the site remained under a sustained DDoS attack. Writing as the attacks were under way, security consultant Dancho Danchev believed it “ smells like a three letter intelligence agency’s propaganda arm has managed to somehow supply the creative for the defacement of Georgia President’s official web site, thereby forgetting a simple rule of engagement in such a conflict- risk forwarding the responsibility of the attack to each and every Russian or Russian supporter that ever attacked Georgian sites using publicly obtainable DDOS attack tools in a coordinated fashion.”[13]Bill Woodcock, the research director at Packet Clearing House, a California-based nonprofit group that tracks Internet security trends, noted that the attacks represented a landmark: the first use of a cyber attack in conjunction with an armed military invasion.[14]

The nature of cyber attacks is such that, two and a half years later, there is still no definitive answer on who caused the attack. They certainly emanated from Russia, but the precise role of Moscow’s military and intelligence services remains unclear. Given that the cyber attacks preceded and accompanied conventional military attacks, there appears to be a link to the Russian government. A March 2009 report by Greylogic “ concluded Russia’s Foreign Military Intelligence agency (the GRU) and Federal Security Service (the FSB), rather than patriotic hackers, were likely to have played a key role in coordinating and organizing the attacks.” They added, “ The available evidence supports a strong likelihood of GRU/ FSB planning and direction at a high level while relying on Nashi intermediaries and the phenomenon of crowd-sourcing to obfuscate their involvement and implement their strategy.”[15]

United States

In a 2010 essay for Foreign Affairs, Lynn revealed that

in 2008, the US Department of Defense suffered a significant compromise of its classified military computer networks. It began when an infected flash drive was inserted into a US military laptop at a base in the Middle East. The flash drive’s malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the US Central Command. That code spread undetected on both classified and unclassified systems, establishing what amounted to a digital beachhead, from which data could be transferred to servers under foreign control.[16]

The upshot is that “ adversaries have acquired thousands of files from US networks and from the networks of US allies and industry partners, including weapons blueprints, operational plans, and surveillance data.”[17]

Lynn classified this attack as “ the most significant breach of US military computers ever” and stated that it “ served as an important wake-up call.”[18]He acknowledged that “ to that point, we did not think our classified networks could be penetrated.”[19]The result of this new awareness was Operation Buckshot Yankee, a fourteen-month program that rid US systems of the agent. btz worm and “ helped lead to a major reorganization of the armed forces’ information defenses, including the creation of the military’s new Cyber Command.”[20]

United Kingdom

In a speech at the 2011 Munich Security Conference, British foreign secretary William Hague revealed that a series of cyber attacks on his country took place the previous year. He noted that “ in late December a spoofed email purporting to be from the White House was sent to a large number of international recipients who were directed to click on a link that then downloaded a variant of ZEUS. The UK Government was targeted in this attack and a large number of emails bypassed some of our filters.”[21]

Additionally, sometime in 2010 “ the national security interests of the UK were targeted in a deliberate attack on our defense industry. A malicious file posing as a report on a nuclear Trident missile was sent to a defense contractor by someone masquerading as an employee of another defense contractor. Good protective security meant that the email was detected and

blocked, but its purpose was undoubtedly to steal information relating to our most sensitive defense projects.”[22]

Finally, in February 2011, “ three of my staff were sent an email, apparently from a British colleague outside the FCO, working on their region. The email claimed to be about a forthcoming visit to the region and looked quite innocent. In fact it was from a hostile state intelligence agency and contained computer code embedded in the attached document that would have attacked their machine. Luckily, our systems identified it and stopped it from ever reaching my staff.”[23]Still, the prevalence and sophistication of these attacks are a principal reason why cybersecurity and cyber-crime were listed as two of the top five priorities in the UK’s National Security Strategy. [24]

Given the interconnectivity of the Internet, Hague argued that more comprehensive international collaboration is vital, noting that, while “ cyber security is on the agendas of some 30 multilateral organizations, from the UN to the OSCE and the G8,” the problem is that “ much of this debate is fragmented and lacks focus.” He continued, “ We believe there is a need for a more comprehensive, structured dialogue to begin to build consensus among like-minded countries and to lay the basis for agreement on a set of standards on how countries should act in cyberspace.”[25]

US- European Attitudinal Differences

We begin to be able to discern a pattern: The United States and the United Kingdom take cyber security very seriously and view it primarily through the lens of national security. The EU and most Western European members of

NATO see it primarily as a national infrastructure problem. In the run-up to the November 2010 Lisbon NATO Summit, Pentagon officials were pressing very firmly to incorporate a concept of “ active cyber defense” into the revised NATO Strategic Concept. Lynn argued that “ the Cold War concepts of shared warning apply in the 21st century to cyber security. Just as our air defenses, our missile defenses have been linked so too do our cyber defenses need to be linked as well.” However, this notion was firmly rejected by the Europeans, with the French particularly adamant.[26]

USCYBERCOM

A July 2010 Economist story proclaimed: “ After land, sea, air and space, warfare has entered the fifth domain: cyberspace.”[27]It noted that President Obama had declared the digital infrastructure a “ strategic national asset” and had appointed Howard Schmidt, the former head of security at Microsoft, as the first cybersecurity tsar. Peter Coates notes that the air force had actually anticipated this move in December 2005, declaring cyber a fifth domain when it changed its mission statement to “ To fly and fight in air, space, and cyberspace.” In November of the following year, it redesignated the 8th Air Force to become Air Force Cyberspace Command.[28]

In May 2010 the Defense Department launched a new subunified command, United States Cyber Command, with Gen. Keith Alexander dual-hatted as its chief while continuing on as director of the National Security Agency. CYBERCOM is charged with the responsibility to “ direct the operations and defense of specified Department of Defense information networks and prepare to, and when directed, conduct full spectrum military cyberspace

operations in order to enable actions in all domains, ensure US/ Allied freedom of action in cyberspace and deny the same to our adversaries.”[29]

As the scale of cyberwarfare’s threat to US national security and the US economy has come into view, the Pentagon has built layered and robust defenses around military networks and inaugurated the new US Cyber Command to integrate cyber-defense operations across the military. The Pentagon is now working with the Department of Homeland Security to protect government networks and critical infrastructure and with the United States’ closest allies to expand these defenses internationally. An enormous amount of foundational work remains, but the US government has begun putting in place various initiatives to defend the United States in the digital age.[30]Even with stepped-up vigilance and resources, Lynn admits, “ adversaries have acquired thousands of files from US networks and from the networks of US allies and industry partners, including weapons blueprints, operational plans, and surveillance data.”[31]

The cyber policy of the United States is rapidly evolving, with major developments under way even as I write this essay. The White House issued a new International Strategy for Cyberspace in May 2011. While not by any means moving away from a defense-oriented posture- indeed, it generated breathless commentary by declaring the right to meet cyber attacks with a kinetic response- it sought to bring commercial, individual, diplomatic, and other interests into the equation. This was followed by a new Department of Defense cyber strategy in July 2011, which built on Lynn’s Foreign Affairs essay.

European Network and Information Security Agency (ENISA)

While CYBERCOM is the most powerful and well-funded US cyber agency, the lead EU cyber agency is ENISA, the European Network and Information Security Agency. Whereas CYBERCOM is run by a general with an intelligence background, ENISA is run by a physics professor with long experience in the IT sector, including the “ energy industry, insurance company engineering, aviation, defense, and space industry.”[32]The agency’s mission is to “ develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organizations in the European Union.”[33]

In December 2010 ENISA released a report identifying what it sees as the top security risks and opportunities of smartphone use and gives security advice for businesses, consumers and governments. The agency considers spyware, poor data cleansing when recycling phones, accidental data leakage, and unauthorized premium-rate phone calls and SMSs as the top risks.[34]New regulations are proposed that would see the perpetrators of cyber attacks and the producers of related and malicious software prosecuted, and criminal sanctions increased to a maximum two-year sentence. European countries would also be obliged to respond quickly to requests for help when cyber attacks are perpetrated, and new pan-European criminal offences will be created for the “ illegal interception of information systems.” Home affairs Commissioner Cecilia Malmström added that criminalizing the creation and selling of malicious software and improving European police cooperation would help Europe “ step up our efforts against cybercrime.”

ENISA’s new mandate will let the agency organize pan-European cybersecurity exercises, public- private network resilience partnerships, and risk assessment and awareness campaigns. ENISA’s funding will also be boosted, and its management board will get a “ stronger supervisory role.” ENISA’s mandate is also to be extended by five years to 2017. The new directive will also supersede a 2005 council framework decision on cybercrime because that previous regulation did not focus sufficiently on evolving threats- in particular, large-scale simultaneous attacks against information systems, such as Stuxnet, and the increasing criminal use of botnets. Stuxnet was recently used to attack Iran’s nuclear power infrastructure, and a single botnet, Rustock, is estimated to be responsible for two-fifths of the world’s spam.[35]

Additionally, EU states are constrained by Directive 95/ 46/ EC, better known as the Data Protection Directive, which provides enormous protection for “ any information relating to an identified or identifiable natural person.” Compare this to the USA Patriot Act, which gives enormous leeway to US law enforcement and intelligence agencies to access electronic data held by US companies in order to investigate and deter terrorist activities. In June 2011 Gordon Frazer, managing director of Microsoft UK, set off a firestorm when he declared that European customer data stored on cloud computing services by companies with a US presence cannot be guaranteed the protections afforded under the Data Protection Directive, setting off a demand from some EU lawmakers to resolve this issue.[36]

Germany

In late February 2011 Germany's outgoing minister of the interior, Thomas de Maizière, unveiled the country's Nationale Cyber-Sicherheitsstrategie (National Cyber Security Strategy).[37]To American eyes, the fact that it was the interior ministry, not the defense ministry, issuing the strategy is striking. It was no accident: this is by no means a defense document.

The document's introduction notes that " in Germany all players of social and economic life use the possibilities provided by cyberspace. As part of an increasingly interconnected world, the state, critical infrastructures, businesses and citizens in Germany depend on the reliable functioning of information and communication technology and the Internet." Among the threats listed: " Malfunctioning IT products and components, the break-down of information infrastructures or serious cyber attacks may have a considerable negative impact on the performance of technology, businesses and the administration and hence on Germany's social lifelines." Contrast this with Lynn's analogy of biplanes over France, and his pondering " at what threshold do you consider something an attack?"

German security scholar Thomas Rid laments that the strategy is " coming a bit late" and that Germany's thinking lags that of the United States and the United Kingdom. Beyond that, he notes that the two agencies created to manage cyber issues are woefully understaffed and tasked with myriad responsibilities related tangentially at best to cyber security. And, according to a cyber " kodex" established in the new strategy, " German interests in data security … would be pursued in international organizations such as the

UN, the OSCE, the European Council, the OECD, and NATO- in that order.”[38]

United Kingdom as Outlier

As is frequently the case on matters of international security, the United Kingdom is much more in line with its American cousin than its neighbors on the Continent. In an October 12, 2010, speech at London’s International Institute for Strategic Studies, Iain Lobban, director of GCHQ (the UK’s National Security Agency analogue, responsible for signals intelligence) noted that his country combines the intelligence and information assurance missions in a single agency, an arrangement “ shared by only a few other countries, most notably the US. It gives us a richer view of vulnerabilities and threats than those who consider them purely from the point of view of defense.”[39]

He confessed to constant barrages of spam, worms, “ theft of intellectual property on a massive scale, some of it not just sensitive to the commercial enterprises in question but of national security concern too,” and all manner of other attacks that have caused “ significant disruption to Government systems.” Consequently, his government was looking to significantly increase its investment in the cyber realm even at a time when the global recession was forcing significant austerity in other departments, including in more traditional military assets.[40]

Thomas Rid notes the sheer breadth of Lobban’s focus: “ Cyber encompasses, for instance, more and more online government services (read: steadily increasing vulnerability); critical national infrastructure,

publicly or privately run; online crime in all its facets; espionage (both industrial and governmental), and such things as the “ proper norms of behavior for responsible states.”[41]

The implications are vast, as Lobban hints and Rid explicates: “ partnerships of a new kind are needed to deal with cyber threats and risks. International partnerships, with like-minded countries that need to establish and maintain appropriate norms of behavior in crisis situations- and intersectoral partnerships, between government agencies and industry, especially the high-tech sector.”[42]

In his Munich Security Conference speech, Hague noted that “ we rely on computer networks for the water in our taps, the electricity in our kitchens, the ‘ sat navs’ in our cars, the running of trains, the storing of our medical records, the availability of food in our supermarkets and the flow of money into high street cash machines.” Further, “ Many government services are now delivered via the internet, as is education in many classrooms. In the UK, 70 percent of younger internet users bank online and two thirds of all adults shop on the internet.”[43]

Given the new awareness of vulnerabilities and the degree of dependence, then, the United Kingdom’s new National Security Strategy “ ranks cyber attack and cyber crime in our top five highest priority risks.” This is not lip service. At the same time that the British military is suffering such severe cutbacks that the Royal Navy is reduced to sharing a single aircraft carrier with France, the current budget “ provided £ 650 million of new funding for a national cyber-security program, which will improve our capabilities in cyber-

space and pull together government efforts.” As part of that effort, Hague said, “ We have established a new Ministerial Group on cyber security which I chair. And we have boosted the UK’s cyber capabilities with the establishment of a new Defense Cyber Operations Group, incorporating cyber security into the mainstream of our defense planning and operation.”[44]

NATO Responses

After months of study and debate the 2010 NATO Summit in Lisbon issued a new strategic concept on November 19, 2010. In it, cyber issues were officially recognized for the first time as a core alliance mission. Recognizing that “ cyber attacks are becoming more frequent, more organized and more costly in the damage that they inflict,” NATO pledged to “ develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defense capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations.”[45]

This was followed in June 2011 by a revised NATO policy on cyber defense and a parallel cyber defense action plan. Combined, they “ offer a coordinated approach to cyber defense across the Alliance with a focus on preventing cyber threats and building resilience.” Additionally, “ all NATO structures will be brought under centralized protection.”[46]

What practical actions will flow from these policy statements remains unclear, especially in an era of radically declining budgets. But they give an overview of what it terms “ NATO’s principle cyber defense activities.”[47]

Coordinating and Advising on Cyber Defense

The cyber-defense policy was implemented by NATO’s political, military, and technical