



GEORGETOWN UNIVERSITY PRESS

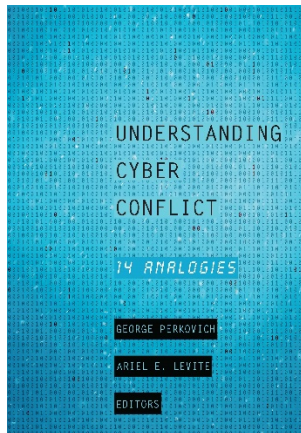
Crisis Instability and Preemption: The 1914 Railroad Analogy

Francis J. Gavin

From *Understanding Cyber Conflict: Fourteen Analogies*

George Perkovich and Ariel E. Levite, Editors

Published by Georgetown University Press



For additional information about the book:

<http://press.georgetown.edu/book/georgetown/understanding-cyber-conflict>

7 Crisis Instability and Preemption

THE 1914 RAILROAD ANALOGY

FRANCIS J. GAVIN

If the first historical analogy American policymakers and pundits reach for during a foreign policy crisis is the 1938 Munich Agreement, international relations scholars are more likely to cite the July crisis of 1914.¹ Many of our most powerful concepts—the offense-defense balance and the security dilemma, misperception and inadvertent escalation, the cult of the offensive and preemptive and preventive war, to name a few—draw heavily on what is believed to be the historical lessons of the European political crisis that exploded into the First World War more than a hundred years ago.²

The role of new technologies, especially the massive expansion of rail lines throughout Europe and their ability to move huge numbers of men and weapons more quickly to the battlefield, is often seen as a key element of how the July 1914 Crisis began and played itself out in a catastrophic world war. Can we generate insights from this history into how emerging cyber capabilities might affect great power crises in the future? What, if anything, can the story of railroads and their effect on international stability tell us about cyber's influence on crisis stability today?

To answer these questions, we must first explore both what actually happened during the July crisis and what the consumers of this analogy *believe* happened. Over time, many aspects of the July crisis analogy have worn thin as historical scholarship has provided a more nuanced view of the origins of the First World War.³ Older notions of the war being inadvertent, driven by miscalculation, or caused by strict adherence to mobilization schedules—in which the function of railroads was crucial—have been challenged.⁴ That said, comparing the two new technologies and assessing their influence on crisis management and stability are revealing, and the work may provide ideas for how to minimize the dangers posed by cyber capabilities in a conflict.

Historical Analogies and the July Crisis

Historians have mixed feelings about analogies. First, historians are often skeptical of the methods other social scientists use to define, identify, cumulate, and explain past phenomena. Even if events can be coded correctly, we are wary of

making predictions. There are far too many omitted variables and confounding factors to meaningfully compare contemporary events, to say nothing of technologies, separated by over a century. Historians would be thrilled if they could explain important single point events or even aspects of bigger questions (such as how railroads influenced decision-making during the July crisis). They point out that the effort to derive generalizations often sacrifices complexity and context.⁵ Another reason historians are ambivalent about analogies is they update their understanding of past events. Many analogies that international relations scholars use, especially surrounding the First World War, are based on long-since contested accounts of what happened during the July crisis. Many international relations scholars still base their analogies on the work of the West German historian Fritz Fischer, despite that professional historians have contested and even discredited many of his arguments.⁶

Recognizing these shortcomings, using well-thought-out historical analogies can still be worthwhile. Human beings reason through analogies, and policymakers often reach for analogies from the past to make sense of the present. Ernest May and Richard Neustadt once suggested that it was like teenagers and sex education: teens are going to do it, so why not help them do it better and more safely?⁷

While there is little consensus on the short- and long-term causes driving World War I, the facts behind the July crisis are well understood. On June 28, 1914, Archduke Franz Ferdinand, the heir to the Habsburg throne, and his wife, Sophie, were assassinated by Gavrilo Princip in Sarajevo, Bosnia.⁸ Princip and his accomplices were part of a secret, pan-Serb organization that sought to expand Serbia's territory and pry Bosnia away from Austria-Hungary. Soon it became clear the attack was undertaken with the knowledge and complicity of high-ranking members of the Serbian government, especially its notorious head of intelligence, Dragutin Dimitrijević, otherwise known as Apis.

A faction led by the Austria-Hungarian military chief of the general staff Count Franz Conrad von Hötzendorf believed the appropriate response was to crush Serbia once and for all. Serbia's territory—and, many thought, its irredentist ambitions—had increased after winning the Balkan Wars in 1912 and 1913. Others, particularly Prime Minister of Hungary Count István Tisza, wanted to avoid a war. In the end, after a drawn-out debate (over three weeks) but with strong backing from Germany assured, the dual monarchy issued a harsh ultimatum to Serbia that any sovereign state would have found difficult, if not impossible, to comply with.

Throughout July each of the major European powers engaged in intense deliberations, diplomacy, and signaling within their governments, among their allies, and with their adversaries. Austria-Hungary would not move without Germany's support, which it received. Both hoped to keep the crisis localized to the Balkans. Russia, however, saw itself as the protector of Slav interests and was wary of Habsburg designs in the region. Still stung by Austria-Hungary's 1908 annexation of Bosnia-Herzegovina, Russia refused to stand by and allow its client, Serbia, to be humiliated. Russia understood, however, that a clash with Austria-Hungary likely meant a war with Germany. France, worried about Germany's

economic and military rise and always seeking an opportunity to reclaim Alsace and Lorraine, backed Russia. Germany swung between aggressive rhetoric and desires to launch a war to fears and concerns about the consequences of a global conflict. Great Britain remained uncertain until the end, fearing German power and intentions, yet at times unenthusiastic over its commitment to alliance partners France and Russia.

It is almost impossible to sort out the vast array of short- and long-term drivers and how they combined to turn the crisis into a world war. Each of the major players was dealing with sharp domestic-political crises that both distracted the government and may have provided a reason to see the July crisis as a welcome diversion. Longer term, the Anglo-German naval race, the imperial competition, the rise of nationalism, the decline of the Ottoman and perhaps the Austria-Hungarian Empires, and the perceived increases in German and Russian economic and military capabilities all generated great instability, as did demographic pressures and ideological clashes.

Europe, however, had weathered almost constant crises and instability in the decade before the outbreak of war in 1914. In addition to arms races between the powers, the First Moroccan Crisis of 1905–6, the Bosnian Crisis of 1908–9, the Second Moroccan Crisis of 1911, and the Balkan Wars in 1912 and 1913 had been very dangerous affairs but had not resulted in a world war between the powers. Tensions were high, but diplomacy worked in each. Cooler heads prevailed, and a global conflagration was avoided. Why was the July crisis different?

Understandably, scholars have focused on the dynamics of the July crisis itself to determine an explanation. Perhaps no country wanted a war, it has been suggested, but perhaps did something about the military environment make escalation more likely and world war unavoidable?

This is where railroads come in. Railroads had first been developed in Great Britain in the early nineteenth century when steam power and innovations in materials used for wheels, wagons, and rails combined to make rail transportation possible. Rail transport was soon competitive with and quickly overtook horse-drawn wagons and canals. Its innovations spread quickly to Western Europe and North America (as well as some European colonies and Latin America) and were key drivers of massive industrialization, urbanization, and economic growth. A century after they were first developed, tens of thousands of miles of rail sprawled throughout Europe, with the capacity to move massive amounts of people and goods in relatively short times. They were widely welcomed as a transformative technology that revolutionized transportation and, with it, society and the global economy.

The military application of railroads was likely first understood and exploited by Germany (as early as in Prussia in the 1840s). Planning for railways and developing war plans against potential adversaries became viewed as connected. Prussia's successful use of rail during its surprisingly quick victories in the wars of German unification between 1864 and 1871 convinced other European countries, especially France and Russia, of the need to better utilize this technology to secure their own national security interests. After 1871 the pace of rail construction

intensified, and the technology of rail improved, all while European nations became increasingly cognizant of rail's potential military uses. Railways were also seen as a way to connect sprawling colonial possessions and increase national influence over wide territories. Germany's construction of the Berlin-to-Baghdad railway, for example, was considered a blatant effort to exercise influence in the Near and Middle East and to threaten especially Russian and British interests.⁹

As European tensions increased in the first decade of the twentieth century, Germany designed and adapted a war plan initiated by the chief of the Imperial German General Staff, Field Marshall Alfred von Schlieffen. Developed for numerous scenarios, the most interesting and ultimately relevant part of the plan crafted in 1905 and 1906 (and updated several times before 1914) envisioned moving quickly with most of the German army and knocking France out of the war before turning against Russia. The plan's success would be predicated on Germany's ability to mobilize and move its armies quicker than France and much faster than Russia could. A smaller German force in the east, cooperating with Austria-Hungary, would stay on the defensive against Russia until France could be defeated and forces moved by rail from the western to the eastern front. France and Russia, however, had their own plans to increase both the size and speed of their respective mobilizations. Russia also planned to massively increase the number and quality of its railways.

Perhaps coincidentally, after 1870 the railroads became more important at the same time political tensions and geopolitical competition increased. The competing military plans and the role of railroads in them also had potential short-term and longer-term consequences for crisis stability. First, if Germany were to prevail in a two-front war with France and Russia, it would have to mobilize rapidly vis-à-vis its potential adversaries. In a crisis, each country would have powerful incentives to mobilize its troops and railways first. If Germany waited too long and France and Russia gained enough of a head start on mobilizing, the former's plans for victory would be undermined. Given that these plans were not a surprise in 1914—Germany's war plans were an open secret—all sides had great incentives to launch their forces preemptively and gain advantage or nullify the advantage over adversaries. This situation had the potential to escalate a middling political crisis into a full-blown clash of arms. The pressure on the European powers to mobilize would be enormous, thereby shortening the time horizons for diplomacy and negotiations to work. Once one side or the other thought conflict likely, it had little incentive to hold back. Worse still, these mobilization plans relied on very rigid, tightly planned movements over railways. Once implemented, hundreds of thousands of troops would be moved forward in ways that would be hard to reverse or alter. The plans of different states appeared to be interlocking; that is, once one country had mobilized its armies and sent them over rail, others had to implement their own mobilization plans lest they be open to defeat.

A longer-term strategic issue also involved railroads. Germany's faith in its military plans was based on its comparative advantages in the size of its army and the speed with which it could move it to the fronts, and the latter was based

in no small part on the quantity and quality of its railways in 1914. German planners recognized that their lead, however, might not last forever. France and especially Russia had ambitious plans to increase and improve their railways and thus nullify Germany's mobilization advantages. German leaders feared that in a crisis several years later, after France and Russia had implemented their plans, the mobilization edge they possessed in 1914 would vanish.

In other words, scholars have suggested that Germany saw a closing "window of opportunity" to exploit its mobilization-railroad advantages, which were a "wasting asset." If war between Germany and France and Russia were inevitable, the Germans might reason, wouldn't it be better to have it take place when Germany still possessed comparative advantages in mobilization power and speed, on which its whole plan for victory was based? If war was sure to come, wouldn't now be better than later? Such thoughts, scholars have suggested, would certainly have influenced German thinking during the crisis, thus making Kaiser Wilhelm II's regime far more willing to take political actions that risked war. The pressures behind mobilization were further intensified by what was known as the "cult of the offensive."¹⁰ Many (though by no means all) decision makers believed there were military advantages to going first and striking a knock-out blow. The spirit of the offensive was also seen as an important part of building a passionate national identity.

In sum, the rapid mobilization and movement to the front of mass armies were made possible in large part by railroads. Railroads, according to the analogy, were destabilizing technologies that made a crisis more likely to escalate toward war. By playing into nationalist ideologies about the ease of the offensive, by decreasing the time and motivation to engage in long, drawn-out crisis management and diplomacy, and by providing powerful incentives to create and implement preemptive military strategies, railroads helped undermine efforts to localize the Balkan crisis and avoid world war. Are lessons here for considering cyber and its influence on great power competition, crisis dynamics, and the outbreak of war?

Similarities and Differences between Cyber and Rail

How are emerging cyber technologies similar to and different from railroads in influencing questions of war and peace? Four similarities and several differences stand out.

First, both rail and cyber are often more commonly understood as "facilitating" technologies. It is accurate that cyber capabilities can be weaponized in ways that can be massively disruptive—for example, by disabling military platforms on the ground and in the air, as well as by potentially crippling an adversary's command-and-control operations. That said, cyber's true strength likely manifests itself when combined with other kinetic capabilities. Alone, neither rail nor cyber are the most powerful, destructive instruments of violence to ensure success on the battlefield, especially in a long, drawn-out conflict. Even when cyber attacks are especially disruptive, their consequences may be temporary or

reversible in ways that conventional attacks often are not. Thus, many cyber capabilities are unlike other technological breakthroughs—for instance, the battleship, the bomber, the tank, or nuclear weapons—that directly and dramatically influenced the intensity and effectiveness of killing the enemy (both his military and civilian populations) and physically destroying his military assets. Rail and cyber technologies may be most effective when they improve military operations in conjunction with more traditional weapons.

An adversary with powerful cyber technologies but impoverished kinetic capabilities can certainly cause damage and create complications for the United States or other cyber-dependent powers. It may also impede, for a time, US progress on a battlefield; however, in the end, it is unlikely to determine outcomes on the battlefield without other technologies or military forces. Cyber alone, for instance, cannot invade or occupy a country. While comparative differences in rail capabilities (namely, speed and volume) certainly mattered, what and whom the railways delivered to the battlefield—the quantity and quality of the soldiers and their weaponry—proved decisive. As with railways, any assessment of potential adversaries' cyber capabilities must be done in a holistic way and consider connections to other assets.

Second, both rail and cyber have thrived as revolutionary civilian technologies that were motivated by and then transformed the economic landscape. Railways are part of what might be considered as the second transportation revolution (with long-distance navigable European ships being the first and aircraft being the third). Domestically, rail replaced horse-drawn transport and canals as the primary means of moving commercial goods. In the process, the cost of shipping goods fell markedly as the distance and volume of goods shipped increased dramatically. This led to tremendous economic growth and increased prosperity in Europe and North America. Similarly, cyber is the key part of what has been recognized as a profound revolution in telecommunications. The ability to move massive amounts of information quickly and at a fraction of previous costs has generated enormous wealth throughout the world.

Why does this matter? Rail and cyber are dual-use technologies with both civilian and military applications that are sometimes hard to distinguish. Undoubtedly the more destabilizing aspects of both rail and cyber technologies were underplayed or underestimated during the early years of each technology revolution. In particular, the military applications of these tools were poorly understood. The opposite worry, however, might be greater cause for concern. Certainly some cyber capabilities are meant purely for coercive or military purposes; for example, the weaponized payload of a virus like Stuxnet obviously has no civilian purposes. Distinguishing civilian from nefarious cyber capabilities ahead of time, however, can be challenging. Many cyber capabilities fall into a murky area, and it may be hard to identify them as “weapons” prior to their use. While measures to limit the dangers and vulnerabilities presented by cyber are eminently sensible, these measures would be ill advised if they undermined or dramatically impeded the enormous economic benefits brought by the information revolution. More work is needed to effectively distinguish and understand

where on what might be considered a spectrum of malevolence—from entirely benign uses to primarily cyber weapons—a potential adversary’s cyber capabilities lay.

Third, both technologies are products and enhancers of the process of globalization. Railroads and cyber have shortened distances, both physical and non-physical, and compressed time by eliminating or reducing intermediary processes. In other words, goods, ideas, and intelligence could be delivered far faster. Political institutions that had developed to deal with more slowly evolving movements may have been challenged by reductions in time. Their decision-making could be compromised by new, unexpected realities, leading more easily to mistakes, accidents, misunderstandings, and misperceptions.

With railways and cyber, this globalizing process led to increased connections, drawing states and societies into closer contact and often obscuring long-held borders and boundaries. Thus, in both cases the issue to focus on is not the technology per se but rather the consequences of the globalizing process on international stability and crisis dynamics. There are two schools of thought on globalization and war. Many believe that the greater interdependence brought by globalizing technologies increases the possibilities of peace, as nations have a greater economic stake in each other. Furthermore, disappearing borders displace entrenched social, ethnic, and economic groups and create constituencies whose identities and interests transcend the prejudices of nationalism. A darker view posits that dislocations attendant to disruptive technologies within states, plus increased exposure and interaction between national groups, can generate greater opportunities for friction between states and increase the chances for conflict.¹¹ The same factors that drive growth and interdependence also expose critical vulnerabilities and weaknesses. Intuitively, the first, more optimistic view of technologically driven globalization holds great appeal. But greater interdependence did not prevent the First World War, and globalizing information technologies today often empower illiberal and destabilizing forces such as the Islamic State.

Fourth, both rail and cyber are compressive technologies. Each, in their own way, condenses the effects of space and time. This is not to say one can neglect the enormous lead time needed to design and construct both rail and cyber platforms, and to plan for their use. When deployed for battle, however, both rail and cyber can dramatically intensify the pace of battle. The speed and carrying capacity of rail moved people farther in far shorter times than in the past. The world became smaller and faster. Cyber has a similar effect. Massive amounts of information and communications can be moved instantaneously with no regard for distance or geography. Space and time are key variables in military conflicts, and this rapid compression might dramatically increase the pressures on decision-making during a crisis.

What are some differences between cyber and rail and their influence on crisis stability and war? The biggest difference surrounds the question of mobilization. With railroads, it is fairly clear who mobilizes, how they mobilize, and for what purpose. Furthermore, what mobilization looks like is obvious: railroads

carry massive numbers of soldiers and matériel to the front according to a strict time line. With cyber, however, the details of who, how, for what purpose, and appearances are far less clear.

Railways were built and are operated out in the open for all to see. A nation's rail capabilities are impossible to hide. To the extent they are part of a military balance of power, they are relatively easy to measure and compare. Rail lines and rolling stock are overt and expensive assets, have large physical footprints, and are relatively transparent and predictable in how they can be deployed. Smart intelligence agencies can study and evaluate them to learn an adversary's capabilities and intentions. When, where, and how railways are built, for example, may provide important clues to what a state is interested in and what its intentions are. A massive buildup of rail capacity to a border, for example, would be an obvious sign and would allow a state to prepare and perhaps initiate defensive countermeasures.

Railways are also a relatively rigid, binary, linear capability. The direction and size of railroads cannot be changed quickly, easily, or secretly. Once a rail-based strategy is launched, it is hard to adapt or change. In many ways, it is a quite predictable capability; railroads, once understood and measured, rarely surprise. Railroads also do not have an attribution problem; when they aid a military action, it is clear where the train originates and where it is going. While a surprise attack may still be possible, an anonymous attack by rail is not.

Finally, railroads are the ultimate manifestation of state power. The rise of the modern nation-state went hand in hand with the rise of rail, which also reflected the ability of the state to generate and mobilize significant resources.

Cyber technologies, in contrast, can easily become tools employed by non-state actors and in fact may reflect the relatively decreased importance of the nation-state in world politics. Furthermore, cyber capabilities exhibit far less observable physical footprints than railroads do. Computer hardware, or physical assets, are obviously involved in cyber activities; however, this technology is usually far smaller, more portable, and more easily hidden than rail technology is. Cyber capabilities can be developed and implemented covertly, unlike railroads. Even if one could locate, identify, and properly evaluate the hardware capabilities of an adversary, the conclusion would largely miss the mark. The key determinant of cyber capabilities is software, both in terms of the computer programs developed and the human talent that produces and operates it. It is extraordinarily difficult to accurately measure cyber capabilities before they are used and even harder to evaluate the balance of cyber capabilities among actors.

Cyber technologies are also flexible and adaptable, ever changing in both peacetime and war, thus making a priori assessments of an adversary's cyber strength very challenging. Cyber attacks can be finely calibrated, making it hard to know how much of a capability is being revealed and making escalation dynamics trickier to predict. As mentioned, both railroads and cyber are dual-use capabilities with civilian and military purposes, and it may be difficult to assess with 100 percent accuracy when they are being used for good or ill. Once railroads are converted to military purposes, however, the shift is clear and, as

noted, tough to reverse. Cyber capabilities exist in a more liminal space, where they can shift quickly, easily, and without detection back and forth between military and civilian uses. Adversaries have powerful incentives to hide the true intent of their capabilities and to make the line between cyber capabilities and cyber weapons murky. The origin of a cyber attack is far easier to hide; thus, one can imagine cyber attacks where the perpetrators are never identified.

The analogy between railroads and cyber capabilities and their influence on crisis stability is, at best, an imperfect fit. A recent high-level study produced by Booz Allen instead explored historical analogies that focused on transnational actors and problems of the global commons. Nuclear nonproliferation, infectious disease outbreaks, food safety in the United States, wildfire suppression, and the response to the 2004 tsunami disaster—all were seen as appropriate cases to mine for historical lessons to deal with cyber attacks.¹² The July crisis was nowhere to be found.

Furthermore, unanswered questions still surround the analogy between rail and cyber and their relationship to conflict. How high are the barriers to entry for both rail and cyber, and how hard is it for states to catch up? Railways, once possessed only by great powers, were soon within the reach of almost every state in the world. Will the same eventually prove true for cyber?

Both technologies are integrative; in other words, they allow people within a nation and between countries to come into closer economic, cultural, social, and political contact with each other. What will the consequences of increasing interdependence be?

Scholars also debate how such technologies influence the so-called offense-defense balance. Do these technologies provide a first-mover advantage that makes conflict more likely? Or, like tanks or aircraft, are they also effective at improving a state's capacity to improve its defensive capabilities? Arms control—based on counting and verifying equipment—helped manage fears of offensives by conventional and nuclear forces. But cyber capabilities do not allow such quantification and verification.

Finally, how do these technologies affect geographical calculations? Railways are located in and affect specific physical spaces, and they presumably have greater influence on conflicts between states that share borders. Still, they also helped connect and deepen ties among sprawling global empires. Cyber may be just the latest manifestation of shifting world politics from local and regional to global concerns, a movement that began with the transportation revolution (naval, rail, air, and, more recently, space) and that intensifies with the more recent revolution in telecommunications and computing.

Exploring answers to these questions can be useful in devising policies to manage offensive and defensive cyber warfare capabilities.

Conclusion

There is a danger in focusing on technology to the exclusion of underlying political factors. Railways did not cause World War I, and it is unlikely cyber threats

will create a great power conflict in the years to come. One of the failings of international relations theory has been to focus too much on a particular military technology, assessing whether it makes offense or defense easier and attributing that characteristic to increases or decreases in the chances of war. The great powers were driven to conflict in 1914, however, by underlying political tensions. German ambitions, both at sea and in continental Europe, aroused suspicion all around. France wanted to recapture its lost provinces of Alsace and Lorraine. Austria-Hungary worried about the threat of Serbian nationalism. Russia had ambitions of its own, especially as the Ottoman Empire continued to recede. Combined with a lethal mix of imperialism, nationalism, economic volatility, demographic pressures, and social Darwinism, conflict and crises were constant in the decade before the First World War. Great power war, though obviously regrettable and avoidable, was thus not completely surprising. No doubt the idea that new military capabilities, including railroads, might aid the offensive and make a war short and decisive created a more permissive environment for states to gamble and risk war. Still, the underlying political tensions and rivalries were the cause of the war and should always be the focus of study. The United States, Russia, Ukraine, China, North Korea, Iran, Saudi Arabia, and any other possible adversaries would do well to understand each other's ideological and geopolitical dispositions first, before assessing how certain technologies would make conflict more or less likely.

That said, cyber does possess characteristics that, similar to other technologies in the past, might be especially destabilizing during a political crisis. Three worrisome characteristics stand out.

First, it is often difficult to identify the sources of a cyber event and even more so to measure cyber capabilities before they've been used. Second, cyber capabilities—even as they take time to develop and deploy—may increase the speed of a conflict once started. By compressing the time available to make decisions, cyber can overwhelm institutions, organizations, and individuals who are used to a more deliberate battlefield. Third, cyber capabilities are neither static nor linear. They can adapt as a battle goes on and, in conjunction with other military capabilities, may have multiplier effects in conflict. This can rapidly shift how the battlefield looks. Furthermore, cyber attacks may be oriented in comprehensive ways at the participants' command, control, communications, and intelligence capabilities, blinding either one or all sides to what is actually happening on the battlefield. These qualities may increase the incentive to use cyber preemptively, as there may be large first-mover advantages. These characteristics may also impede war termination or efforts to prevent escalation, as one side or another may lose the capability to assess the battlefield and might assume the worst.

What lessons might the First World War provide? One is struck, looking about over a century ago, at how under-institutionalized Europe was. While massive numbers of soldiers and military equipment could be moved far more quickly, information and intelligence—and the ability to properly assess, share, and deliberate on them—did not seem to keep pace. Not only was there little opportunity for adversaries to discuss conflicts, reveal their intentions, and negotiate

stand-downs but also there was often complete opacity among allies and even within governments. In other words, railways had compressed the amount of time needed to make good decisions, but the political and diplomatic institutions that were part of this process had not advanced. One can imagine a world where the leaders of those great powers had a place and a reason to discuss their differences (i.e., a United Nations), where the allies had a place to better understand and synchronize their political and military strategies (i.e., a North Atlantic Treaty Organization), and where the civilian and military wings of government could better consult and share their plans and could better coordinate and offer a unified national strategy (i.e., a National Security Council). A more deeply institutionalized Europe in July 1914 might not have resolved the deep underlying political tensions driving tension, but it might have prevented their escalating into a catastrophic great power war.

With cyber capabilities, information and intelligence can now move quite quickly, yet the ability to process, assess, share, and deliberate them may not exist. The making of cyber strategy and policy in most countries today appears to be divided up between different groups and disaggregated, still lagging the innovation of capabilities. Cyber represents a technology that, once again, compresses the time available during a crisis to make decisions. Furthermore, cyber capabilities may actually degrade the ability to make such decisions. At the very least, leaders and experts should think about the institutional capacities of states to deal with massively increased amounts of information coming from a variety of different sources and in an environment where cyber attacks might be oriented toward degrading and blinding their capabilities. In other words, while little can be done in the cyber realm to shape larger political dynamics, steps can be taken to lessen the dangers that a cyber attack during a crisis will make war more likely or deadlier.

Notes

1. For the best historical work on how policymakers use and misuse analogies, see Yuen Foong Khong, *Analogies at War: Korea, Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton: Princeton University Press, 1992); and Ernest May, *“Lessons” of the Past: The Use and Misuse of History in American Foreign Policy* (Oxford: Oxford University Press, 1975). While most policymakers do reach for Munich, the July crisis haunted President John F. Kennedy during the Cuban Missile Crisis. See Robert Zaretsky, “Struggling with Destiny: Barbara Tuchman’s Legacy as an Historian,” *TLS: Times Literary Supplement*, February 24, 2012.

2. See, for example, the essays in Steven E. Miller, Sean M. Lynn-Jones, and Stephen Van Evera, *Military Strategy and the Origins of the First World War* (Princeton: Princeton University Press, 1991).

3. For an extraordinary, in-depth review of recent historiography before the recent slate of books, see Samuel R. Williamson Jr. and Ernest R. May, “An Identity of Opinion: Historians and July 1914,” *The Journal of Modern History* 79 (June 2007): 335–87.

4. The centennial of the July crisis of 1914 saw many new works of history on the origins of the First World War. For an overview of the key new works, see Francis J.

Gavin, "History, Security Studies, and the July Crisis," *Journal of Strategic Studies* 37, no. 2 (2014): 319–31.

5. For an excellent example of this view, see John Lewis Gaddis, *The Landscape of History: How Historians Map the Past* (Oxford: Oxford University Press, 2002).

6. Marc Trachtenberg, "New Light on 1914?," July 29, 2015, unpublished paper.

7. Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision-Makers* (New York: Free Press, 1988).

8. This overview is from Gavin, "History, Security Studies."

9. Sean McMeekin, *The Berlin–Baghdad Express: The Ottoman Empire and Germany's Bid for World Power* (Cambridge: Belknap, 2012).

10. Stephen Van Evera, "The Cult of the Offensive and the Origins of the First World War," in Miller, Lynn-Jones, and Van Evera, *Military Strategy*, 59–108.

11. For a comprehensive view of the scholarship on whether, when, and how economic interdependence causes war or peace, see Dale C. Copeland, *Economic Interdependence and War* (Princeton: Princeton University Press, 2014). For a study that focuses on the cultural and civilizational tensions generated by interdependence, see Samuel P. Huntington, *The Clash of Civilizations and the Remaking of World Order* (New York: Simon & Schuster, 1996).

12. Booz Allen Hamilton, *Cyber Operations Maturity Framework: A Model for Collaborative, Dynamic Cybersecurity* (McLean, VA: Booz Allen Hamilton, 2011).