Are we in a Digital Cold War?

Milton Mueller

Presented May 17, 2013 at the GigaNet workshop *The Global Governance of the Internet: Intergovernmentalism, Multistakeholderism and Networks*, Graduate Institute, Geneva, Switzerland.

I first heard the *Cyber Cold War* concept applied to the Internet in the aftermath of the Dubai World Conference on International Telecommunications (WCIT). There, the world's nations seemed to split in half over the future of Internet governance. One writer called it the "Internet's Yalta" (Klimburg 2013). The concept gained momentum with the February 2013 release of a report attributing systematic cyber-espionage to a unit of the Chinese Peoples' Liberation Army (Mandiant 2013). Suddenly we had U.S. cybersecurity firms with direct ties to the American military openly talking about a long term, systematic threat from a foreign power in terms reminiscent of 1960s-era warnings of the communist plan for world domination. Reporters and media outlets echoed the theme. A former CIA head actually compared the use of Stuxnet to Hiroshima.

My initial reaction to this metaphor was viscerally negative. The very act of framing the problem in that way, I thought, contributed to the militarization of the Internet and foreshadowed a bleak future: an Internet policy landscape dominated by national security concerns and great power conflict. But I could not help but start thinking about the parallel. What, exactly, was wrong with characterizing conflicts over cyber space as a Cold War? What, exactly, are the policy implications if we continue to do so? In order to answer those questions one must explore the metaphor, not reject it out of hand.

This led to a change of heart. While I continue to reject the values and policy predilections of the new cold warriors, there is in fact a growing linkage between cyber policies and national security. It is also true that policy conflicts between Internet freedom advocates and advocates of state-centric regulation have enmeshed cyberspace in inter-state conflict. Moreover, on both sides there are interest groups and ideologues who wish to actively promote the equivalent of a digital cold war, which could make it a self-fulfilling prophecy. Those problems will not go away if we refuse to acknowledge or discuss the Cyber Cold War concept. Indeed, ignoring or dismissing the parallel is probably as dangerous as an uncritical acceptance of it.

The best response to the challenge would be a historically informed review of the nature of the Cold War, coupled with a dispassionate analysis of its similarities and differences to the current cyber situation. What can we learn from this comparison?

The Long War

The first insight comes from achieving a deeper understanding of what the Cold War really was. In his book *The Shield of Achilles*, Philip Bobbitt argues convincingly that what we now call the Cold War was really the last episode of an epochal war over the nature and constitution of the 20th century nation-state (Bobbitt 2002). In this perspective, a whole series of conflicts – World War 1, the Bolshevik revolution, the Spanish civil war, World War 2, the US-USSR confrontation, and the Korean and Vietnam wars – were episodes of a single Long War. All of these conflicts "were fought over a single set of constitutional issues that were strategically unresolved" until the 1990 Treaty of Paris brought a formal end to the Cold War. What were these "constitutional issues?" The Long War was fought to determine which of three new, competing forms of the nation-state would replace the 19th century imperial states of Europe: market-oriented parliamentary democracy, communism and fascism.[1]

Gegen Papen, Hitler, Thälmann
LISTE 2
SOZIALDEMOKRATEN

Allegedly fought to "make the world safe for democracy," WW1 did not actually resolve the question of what sort of system would prevail. On the contrary, it nurtured both communism (the Russian revolution) and fascism (most notably, in the German reaction to the Treaty of Versailles). Far from resolving the battle among the constitutional systems, WW1 "only generalized that question to virtually all states." (Bobbitt

[1] In this triadic competition, tactical opportunities routinely led communists and fascists to ally against democrats (e.g., the Hitler-Stalin pact), parliamentarians to ally with fascists against communists (e.g., the White Russians or U.S. support for anti-communist dictators), and communists and parliamentary systems to ally against fascists (e.g., the U.S. and Stalin against Hitler). Still, corroborating Bobbitt's thesis, none of these alliances were durable and each ideological form sought to eliminate the other once the tactical advantages achieved through an alliance were depleted.

2002 p. 27) The Great Depression intensified the competition among these contradictory orders (Berman 2006). By the 1930s, there was not a country in the developed world, and few in the colonial world, that did not have indigenous fascist, communist and liberal-democratic or social-democratic parties.

World War 2 eliminated fascism as a viable option among the great powers. The defeat of Germany, Italy and Japan, however, only produced a bi-polar world. Two great powers representing two distinct ways of constituting the state still stood facing each other tensely in conquered Germany in 1945, dividing Europe in two. They reflected different systems of political economy that were defined as incompatible and mutually exclusive: capitalism and democracy on the one hand vs. socialism, communism, Marxist-Leninism, anti-imperialism on the other. This competition defined international relations for the next 45 years, drawing most states and international processes into it, directly or indirectly.

The Cold War

In the competition between the US and the USSR, it was not the military might of the Soviet Union or even its undemocratic system *per se* that triggered American and British Cold War initiatives. It was, rather, the fear that the Soviet system could capitalize on postwar political upheavals to tip the balance of power decisively in its favor. As Paul Kennedy (1987, 380) wrote of this period,

"[World War 2] had caused immense social and political turbulence…even in countries not directly overrun by invading armies (e.g., India or Egypt). Traditional social orders lay smashed, colonial regimes had been discredited, underground nationalist parties had flourished, and resistance movements had grown up, committed not only to military victory but to political transformation."

The growing popularity of communist parties in postwar Europe and a surge of revolutionary and nationalist movements in the wake left by European colonialism's retreat was increasingly seen by the U.S. as a threat. It feared that the emerging nations and key parts of Europe would align themselves with the communist system in the global competition. Unless the Cold war was actively waged, communist advances would tilt the tense, post-WW2 standoff in the Soviet Union's favor.

Thus, as early as March 1946 Winston Churchill was calling for a diplomatic offensive against the Soviet Union. American diplomats George Kennan and Clark Clifford were calling for measures to contain growing Soviet power and recommending that America "support and assist all democratic countries which are in any way menaced by the USSR," respectively. On March 12, 1947 U.S. President Harry S. Truman's decisively threw the U.S. into the Cold War, declaring that "nearly every nation must choose between alternative ways of life."[2] The new Truman doctrine announced an American foreign policy that would "support free peoples who are resisting attempted subjugation by armed minorities or by outside pressure." American leftist Henry Wallace countered that "There is no regime too reactionary for us provided it stands in Russia's expansionist path. There is no country too remote to serve as the scene of a contest…."[3]

While many aspects of the competition were economic and ideological, technological advances in weaponry played a major role too. The develop-ment of nuclear weapons by the U.S. solidified its status as the dominant power. The strategic advantages that could be obtained from nukes triggered an arms race between the U.S. and Russia, resulting in the production of stockpiles capable of unfathomable destruction. Mutually assured destruction ultimately (and perhaps only luckily) deterred direct military conflict between the two great powers, but it did not prevent conflict in other areas. It fostered hot wars and extensive violence in the contested areas of the world, including devastating conflicts in Korea, Vietnam, Laos, and Cambodia. It was an international system of constant tension, high risks and many wars.

[2] At that moment Truman sought $400 million in economic and military aid to the governments of Greece and Turkey; this massive commitment of resources would go to a right-wing Greek monarch embroiled in a civil war against a communist party supported by Yugoslavia, and to a Turkish Republic worried about Russian pressure to grant free access to Soviet ships through the straits connecting the Black Sea to the Mediterranean.

[3] http://teachingamericanhistory.org/library/index.asp?document=852

The cold war was ultimately won by the liberal capitalist democracies, but not because of its superior military capabilities. It was the inability of socialist planned economies to innovate and produce wealth for its citizens that undermined their legitimacy from within and retarded their growth and military strength (Kennedy 1989, McMahon 2003). From the late 1970s on, the contrast between the material well-being of South Korea and North Korea; between Taiwan and mainland China; between Eastern and Western Europe became increasingly evident. It was also clear that the technological superiority of the West, especially in information technology and telecommunications, had profound military as well as economic implications. Gorbachev's attempt to reform and revitalize the Soviet economy, known as *perestroika*, was an attempt to bridge that gap. Because he had to overcome the resistance of vested interests to achieve *perestroika*, he attempted to open up the political system as well, and that is when things slipped out of his control and the Soviet system began to unravel. So that, by 1990, the second of the three alternative constitutional forms of the modern nation-state was effectively eliminated. This resolved an 8-decade struggle over the dominant constitutional form of the modern state. From this perspective, the Cold War was merely the penultimate episode of the Long War.

War and the transformation of the state

That larger perspective on the Cold War is important to students of internet governance. It calls attention to three salient facts about the current situation.

First, the form taken by the state changes over time, and it changes more frequently than we typically realize. The popular idea that we have been in a "Westphalian" system since 1648 is bad history and bad political science. Bobbitt (2002, 17) challenges this orthodoxy, claiming that:

> *…the nation-state is relatively new - being little more than a century old - and has been preceded by other forms of the state, including forms that long antedated the Thirty Years War. The nation-state is dying, but this only means that, as in the past, a new form is being born.*

The form taken by the state prior to WW1 was very different from the modern nation-states that emerged in the past century. The Westphalian ideal bears little resemblance to the pre-World War 1 empires of Great Britain and Austria-Hungary, the Ottoman empire, imperial Russia and expanding aspirant Japanese and German empires. Internet governance scholars such as myself, who emphasize the way the problems of Internet governance are leading to innovative departures from nation-state governance (Mueller 2002, Mueller 2010), can find support in this view of history. Those who insist, on the other hand, that the problems of Internet governance can only be solved by resorting to the tried and true hierarchies of the classical nation state need to think again. What they present as a re-establishment of the "normal" way of doing things would actually be an exceptional degree of stasis, a bizarre hiatus in the course of political evolution. It is the norm for new technologies affecting military, economic and political power to alter the form of the state.

Second, major changes in the constitutional form of the state are usually accompanied by violent conflict (war, revolutions, and the like), and are correlated with technological innovations in military capabilities. This is to be expected because the state itself is best conceived as a monopoly on the use of legitimate force. If there are competing ideas about the legitimacy or the modes of existence for states, major incompatibilities among them will result in both domestic and international conflict, most probably violent conflict, if they co-exist and overlap across the same society. This means that we need to take the relationship between cyber space and military conflict seriously (at least, analytically) for if the internet and cyberspace do transform war and politics then it is inevitable that they will also transform the nature of the state and disrupt the international system. What we have to look out for, to draw on the old proverb, are generals who are preparing to fight the last war, not the one we might face in the future.

Third, this approach brings into sharper focus one of the elephants in the room in the Internet Governance debates. That is the fact that the younger nation-states – the ones that only just emerged in the post WW2 period – seem to be the most strongly committed to a backwards-looking, sovereigntist or neo-Westphalian approach to Internet governance. In many respects, the battle over the vision of Internet governance cannot be characterized entirely accurately as between authoritarian, undemocratic states and liberal, freedom-loving states, but also and more centrally as a conflict between long-established, cosmopolitan states and newer states still insecure about their sovereignty. In some sense this is understandable. Having achieved independence from the imperial and colonial structures of the West only a couple generations ago, and finally getting “their turn” to run a state aligned with their “nation,” little wonder countries such as Brazil, Russia, India, China and South Africa are concerned with the extent to which an increasingly important sector of the postmodern economy, communication and information, seems suddenly exempt from the classical model of national control. This observation should not, however, be construed as a justification for the sovereigntists. It took the newly independent nations several decades to learn that the socialist and communist ideologies that were effective at mobilizing independence struggles and overthrowing colonialism were disastrously counterproductive as guides to economic policy once they were in power. It may take them another decade or so to learn that the territorial nation-state governance is irretrievably counterproductive in the domain of 21st century communication and information policy.

The comparison considered

With those two factors in mind, what is comparable and what is fundamentally different about the current situation? We look first at China, then at ideological and constitutional polarization, and finally at the question whether cyber capabilities are transforming war.

The case of China

When considering China, it is possible to argue that the Long War never really ended and thus that the Cold War is still ongoing. That is because China, unlike Russia, succeeded in reforming its socialist economy – opening it up to enough market forces to lift its people out of poverty – while successfully retaining a Communist Party monopoly on political power. From a Marxist-Leninist point of view, Deng Xiaoping succeeded where Gorbachev failed. China could be seen, therefore, as an evolved form of the Communist state better equipped to struggle for supremacy with the U.S. militarily and economically. It also promulgates an alternative ideology about the role of information in society, emphasizing aggressive management of public expression, the disruptiveness and undesirability of dissent and disagreement, the goal of a 'harmonious' Internet. China joins many G77 countries pushing for an intergovernmental, sovereigntist approach to Internet policy at the ITU. China is also an emerging great power, building up both its economic capabilities, which will eventually surpass those of the US simply because of its sheer size, and inevitably also its military strength. Has China taken the place of the USSR in a continuation of the Long War? This is about as plausible as the Cyber Cold War case gets. But there are some obvious problems with this scenario.

First, the level of economic integration and interdependence between the U.S. and China greatly undermines the Cold War comparison. The United States is China's top trading partner.[4] If the U.S. economy were destroyed or "taken over" by China somehow, or vice-versa, the economies of both states would be worse off to a degree that would threaten the viability of both. Because the legitimacy of the Chinese Communist Party depends almost entirely on continued delivery of improved standards of living, major damage to the U.S. would constitute an existential threat. Hawkish American talk about China's cyberattacks *assumes* that China is

[4] U.S. goods and services trade with China totaled $539 billion in 2011. U.S. imports from China have been growing at an average of 14% per year since 2001; U.S. exports to China have been growing at an average of 19%/year since 2001.

bent on our destruction and takeover, and then (mis)interprets espionage and intellectual property theft as military acts. In fact, misappropriation of intellectual property from more advanced countries is a time-honored economic development strategy – one used by the U.S. in its early days as well. Short of a real shooting war, it is hard to see how any crippling blow to the U.S. financial and communications infrastructure via cyber attacks would not also inflict severe damage on China's economy as well – even assuming such scenarios were plausible.

Realist international relations theorists don't buy the thesis that economic interdependence will prevent war. But even they believe that two great powers separated by large oceans and armed with nuclear weapons pose little direct military threat to each other (Mearsheimer 2001).

The other problem with this scenario is that it lacks the bi-polarity and exclusivity of the Cold War competition. Neither China's state nor its Internet are seen as a beacon or model that animates and inspires the rest of the world. The rest of the world is not in the liminal state it was in after World War 2, when dozens of new post-colonial governments were being formed. There are no Communist Parties in Japan, South Korea, Thailand, Egypt, Turkey, Greece, Italy or India linked to and supported by the Chinese CP and well-placed to seize power and turn those states into clients or satellites of China. Indeed, China has very few real military allies. Also, it is now more of a multi-polar world. The European Union, Russia, India and others formulate independent political, military and economic responses to China's rise – they do not just huddle under the U.S. security umbrella.

A choice between 'alternate ways of life'?

Is there an ideological division in the world comparable to the capitalism/democracy vs. socialism/ communism dichotomy? In the Internet sphere, yes there is – partially. But a vitally important historical distinction is that *this division is not led or defined by states*.

There is an ideological division around two distinct issues. The first is the appropriate institutional form of Internet governance, the other pertains to the substantive aspects of communications policy. With respect to governance forms, younger states and authoritarian states favor a pre-eminent role for sovereigns in communications policy, and would rely on the negotiation of intergovernmental agreements for global governance. The other side, which is led not by specific states by but private sector actors in the technical community, business, and to some extent civil society, supports the organically developed

Internet institutions (Mueller, 2010), which represent transnational governance and more open, bottom-up, participatory institutional mechanisms.

With respect to the substantive features of communications policy, in transnational civil society in the developed world and in many parts of the middle income or developing world, there is a party of Internet freedom that opposes censorship, surveillance, monopoly and heavy-handed intellectual property protection while supporting innovation, free expression and privacy; on the other side there are states with authoritarian tendencies that want to reassert sovereign power over digital communications in order to protect its local political equilibrium against cosmopolitan disruption. In short, there is a conflict between advocates of individual freedom and state-centric regulation. Usually (but not always) advocates of multistakeholderism align with advocates of Internet freedom and supporters of intergovernmental governance promote more regulation and control of the internet.

But unlike the Cold War, the competition between these different visions of the Internet is not really embodied in, and polarized around, two great power states that seek to draw other nations into mutually exclusive systems of political economy.[5] The US government's attempt to position itself as the standard-bearer of Internet freedom, always dubious, was finished off by the recent revelations regarding NSA surveillance. State-actors who advocate Internet freedom and "the multistakeholder model" are inherently hypocritical. Even when they do not directly contradict themselves, their support for the organic Internet governance institutions seems opportunistic, inconsistent and partial – especially when matters of national interest or national security are involved. One can rarely go wrong adopting a realist perspective when interpreting state actions in Internet governance. States are states, seeking to enlarge and preserve their power, looking out for their own interests. In ICANN's case, U.S. support for the "multistakeholder model" is entirely a function of the fact that ICANN is tethered to the US and provides privileged forms of influence – it is not about substantive policy. On the other hand, the states that resist U.S. hegemony are not revolutionary advocates of a new system of national or global governance, but rigid and conservative forces that want to protect their political status quo from foreign cultural and political influences. So the Cold War metaphor breaks down on both sides of the equation.

What's strikingly new about the current situation is that TCP/IP truly links everyone. States, business and civil society, on all sides of the ideological, political or cultural divides, are part of the internet. A *true* Internet Cold War would mean that the two sides coalesced around alternative data communication protocols. Yet no one is proposing a competing, incompatible data communications protocol that would allow one part of the world to turn off their TCP/IP

[5] One might argue that China and the US meet this criterion, but as argued in the previous section, both are part of the same economic system.

and congregate on a competing standard that shut out the liberal economies.[6] There are firewalls and filters, yes, but no alternate DNS root, no different Internet address registry system. Indeed, it is not just the Internet *per se* that binds together our world of information and communication: so do the 802.11 standards for WiFi; the Windows, Apple and Android operating systems; the device manufacturers in Korea, China, Europe and the U.S. To some extent, so do Twitter, Google and Facebook, all of which are known and missed even when they are actively blocked.

One can hardly overemphasize this aspect of the distinction between the historical epochs. During the Cold War, taking one side literally meant severing diplomatic, economic, technological and social links with the other side. The American-led Intelsat system, for example, was for the West. The Soviets did not join it and complain about its dominance by the U.S. They did not try to get the ITU to "take it over." Rather, they created Intersputnik, an alternate satellite system that wove together the Eastern bloc. Similarly, trade, immigration and travel between East and West was highly restricted. East and West were different economies. Physical walls were built to separate them, and people were shot if they tried to cross them. This isn't happening today.[7]

Cyber weapons

Referring to Stuxnet, a former CIA director, General Michael Hayden said, "This has the whiff of August 1945…Someone, probably a nation-state, just used a cyber weapon in a time of peace…to destroy what another nation could only describe as their critical infrastructure."[8] Are cyber-war and cyber weapons transforming military capabilities, which, as noted

[6] One might, if one wanted to poke fun at the Internet technical community, mention IPv6 as an incompatible data communication protocol that might fragment the world. It is also the U.S. and Europe who are toying with ideas of "doing the Internet over again, only better" with new "clean slate" protocols that will (allegedly) solve all the internet's current problems via improved design. One can only smile in amusement at the implicit design-utopianism here, but at any rate if there is a threat of fragmentation or division it is here.

[7] True, North Korea and Iran are isolated in this manner, but they are small exceptions. The North Korean case is a backwater that has remained stubbornly resistant to the resolution of the Cold War. And both Iran and North Korea use the TCP/IP protocols and are connected, however tenuously, to the global Internet.

[8] Paul Shinkman, "Former CIA Director: Cyber Attack Game-Changers Comparable to Hiroshima," US News, February 20, 2013. http://www.usnews.com/news/articles/2013/02/20/former-cia-director-cyber-attack-game-changers-comparable-to-hiroshima

before, could be the path to a digital Cold War?

No. Hayden either has an agenda or he is out of touch with reality. Cyber weaponry is not a revolutionary factor capable of altering the military competition among states on a global scale. I agree with Thomas Rid that the military aspects of cyber have been grossly overstated (Rid 2013).

Put simply, there have not been any cyberwars yet. The things we call cyber weapons have not brought about a new kind of conflict that has altered the strategic balance among states engaged in military conflict. (Massive Internet-based surveillance may be doing that, but that is another story, outside the scope of this paper.) There is nothing going on comparable to the French innovation of introducing mobile artillery in 1494, leading, in Bobbitt's view, to the end of the princely state and the rise of the kingly, territorial state. There is nothing comparable to nuclear weapons.

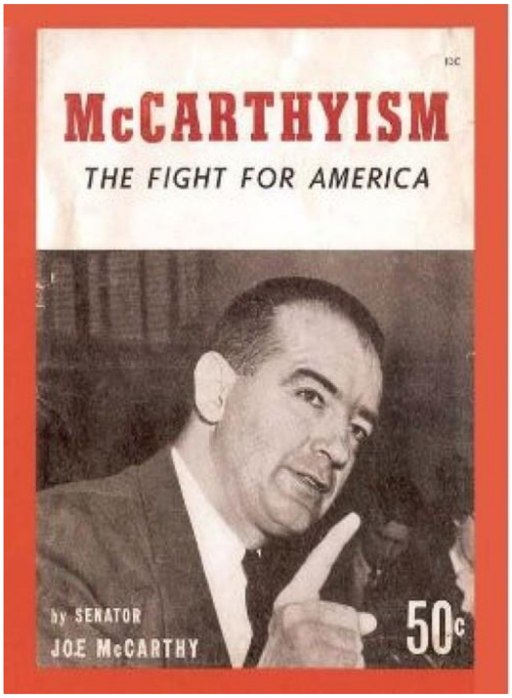
Let’s compare cyber- and nuclear weapons. In a space of only 6 years (1939-1945) a commitment to develop nuclear weapons was made and the weapons were developed, tested and used. Their use not only contributed to the end of WW2, but decisively altered the terms of the ensuing strategic relations among great powers for the next 5 decades. The possession of nukes and ability to deliver them is to this day a major factor defining inter-state power relations, as the controversy over Iran illustrates.

By way of contrast, we have been talking and writing about cyber war for more than 15 years (Arquilla and Ronfelt 2001); in that time no state has been overthrown, no governance capability gained or lost, no realignment of territorial boundaries has ever occurred based exclusively or even primarily on cyber-attacks and cyber weapons. Graham (2012), referring to the 2008 incidents in which Russia is alleged to have attacked Georgia using cyber methods coordinated with military attacks, asserts flatly, "there's no evidence the cyber attacks were by the Russian government, or that they were anything more than normal ‘citizen hacktivism.’” Those “advanced, persistent” Chinese threats we read about in February were aimed at espionage and theft of intellectual property; even if they were state-sponsored, they were not acts of war or anything close to it. They didn’t destroy anything. Terrorists continue to realize their objectives by planting bombs made of pressure cookers and nails, not by attacking the DNS or critical infrastructures through cyber means.

The best example of a cyberweapon we can come up with is Stuxnet, which despite its incredible sophistication as a cyber-exploit, was nothing more than an act of sabotage against a few highly specialized pieces of machinery. The worm was but one small piece of an overall program of economic sanctions, kinetic military threats and diplomatic isolation. And oh, by the way, the Iranian nuclear program is still underway. Comparisons to “August 1945” seem patently absurd.

There can be riots and civil disorder in cyberspace (Estonia); there can be vandalism and social protest (Anonymous); there can be temporary disruption (DDoS attacks by state or nonstate actors); there can be espionage and data theft (APTs from China); there can even be sabotage (Stuxnet). All of them can be influential in one way or another. But so far there is no evidence that any of this can lead to large-scale death and destruction, or that it is capable of altering the strategic balance among the world's states, or that is producing some kind of struggle between alternate forms of the state.

While it is at least conceivable that some yet-to-be-developed cyber activities could be used to wreak large-scale destruction comparable to nuclear missiles or a conventional ground assault, its use is conceivable only in a context where the conflicting powers were engaged in or on the verge of traditional warfare and might just as well use nukes and other kinds of kinetic weapons. Cyber simply does not transform war the way nukes did. It does transform other kinds of power relations, however – and that is the point. We are dealing with something fundamentally different.



Replay

Nevertheless, the structural differences between the Cold War and the present do not prevent the political and mental repertoires it created from being revitalized, creating undesirable political dynamics. Internal to the superpowers the Cold War rewarded political actors who claimed that their government was vulnerable or falling behind in the arms race. Even though the US enjoyed a huge advantage in nuclear missile capabilities at that time, liberal Democrat John F. Kennedy mounted a successful political attack on the outgoing Eisenhower administration by claiming that a “missile gap” existed between the US and the Soviet Union. The prospect of a persistent, globalized competition with another superpower gave hawks a bizarre rhetorical advantage in public debate. With truly existential stakes, and an inherent inability to know with absolute certainty whether or not one is vulnerable until a fight actually begins, many voters and legislators were willing to err on the side of “more” security, no matter how implausible the claims of insecurity. This faction would also be reinforced by economic interest groups who benefited from military expenditures. This dynamic seems to be very similar to what is happening today. One does not even need a single, global superpower competition; similar effects were achieved with the “war on terrorism,” for example.

On the US side, the Cold War tended to conflate liberal ideals with anti-communism; i.e., it subordinated the achievement of liberal freedoms to the task of confronting the spread of

Soviet-backed communism. This involved support for dictators in the developing world so long as they professed to be anti-communist, and the overthrow or subversion of democratically elected but leftist political leaders for fear they would lead countries into the communist camp (Iran, Greece). It also sacrificed or reduced freedom and democracy domestically. The Cold War led to massive expansion in the size of the US state, increased levels of government intervention in key areas of the economy, restricted civil liberty and press freedom, and prolonged the use of conscription – the very things the liberal order was supposed to oppose constitutionally and ideologically. All flowed logically from the permanent state of war or wartime readiness created by the Cold War. The American rightwing – the conservatives who have somehow associated the national security state with rhetoric about "less government" and "freedom" – have been trapped in this dilemma for decades.

Here again, the prospect of a replay is quite real. Cybersecurity threat-mongering actually militates against the Internet freedom agenda of the liberal democratic states. It leads to the concentration and centralization of power (both political and economic) not to its decentralization and diffusion. It prioritizes national security over individual rights and human security; it fuels yet more governmental surveillance and to reductions of due process. It leads to restrictions on open entry and innovation in Internet businesses. It was fascinating to watch the allegedly pro free trade U.S. Government demonize Chinese telecommunications equipment manufacturer Huawei with so little evidence. In this case national security concerns were so perfectly meshed with protectionist economics that one could hardly defend an open equipment market without sounding like an apologist for the Chinese.

Conclusion

When examined honestly, the cold war metaphor does not provide a very good rationale for reasserting traditional forms of nation-state power in the name of cybersecurity. On the contrary, a direct comparison underscores the profound differences in the type of conflict we were facing then and the type we are facing now. It calls attention to the great powers' transcendence of traditional disputes about control and expansion of their territory (due in large part to nuclear weapons) and their economic and technological interdependence.

Whatever the political dangers of reviving a Cold War mentality, its use as a point of comparison can be instructive and useful. It asks us to place geopolitical conflict in a historical context that emphasizes the ongoing transformation of the state caused by new forms of interdependence, weaponry and conflict. It tells us not to re-fight the Cold War, but instead to consider the constitutional implications of what we are actually fighting for – and against.

References

Arquilla, J. and D. Ronfelt, Eds. (2001). Networks and Netwars: The future of terror, crime and militancy. Santa Monica, CA, RAND Corporation.

Berman, S. (2006). The Primacy of Politics: Social Democracy and the Making of Europe's Twentieth Century. Cambridge, Cambridge University Press.

Bobbitt, P. (2002). The shield of Achilles : war, peace, and the course of history. New York, Knopf.

Kennedy, P. M. (1989). The rise and fall of the great powers : economic change and military conflict from 1500 to 2000. New York, Vintage Books.

Klimburg, A. (2013) The Internet Yalta. Center for a New American Security **http://www.cnas.org/theinternetyalta**,

Mandiant (2013). APT1: Exposing One of China's Cyber Espionage Units. Washington, DC, Mandiant, Inc.

McMahon, R. (2003). The Cold War: A Very Short History, Oxford University Press.

Mearsheimer, J. J. (2001). The tragedy of Great Power politics. New York, Norton.

Mueller, M. L. (2002). Ruling the Root: Internet governance and the taming of cyberspace. Cambridge, MA, MIT Press.

Mueller, M. L. (2010). Networks and States: The global politics of Internet governance. Cambridge, MA, MIT Press.

Rid, T. (2013). Cyber war will not take place. Oxford, Oxford University Press.