Center for a New American Security

FEBRUARY 5, 2013

COMMENTARY

The Internet Yalta

By Alexander Klimburg

The December 2012 meeting of the World Conference on International Telecommunications (WCIT) may be the digital equivalent of the February 1945 meeting of the Allied powers in Yalta: the beginning of a long Internet Cold War between authoritarian and liberal-democratic countries. The battles over Internet governance that surfaced at WCIT are not just about competing visions of the Internet, with one side favoring openness and the other security. They are also about two different visions of political power – one in which that power is increasingly distributed and includes non-state actors, and one in which state power is dominant. At the Yalta Conference, Western democracies made two fundamental mistakes: first, they allowed naive statements of wishful thinking to supplant actual realities on the ground. Second, they overlooked the risk inherent in permitting ambiguous definitions. Both of these mistakes may have been repeated at WCIT.

The International Telecommunication Union (ITU) called, and governments answered. Upon invitation of the ITU, an independent agency of the United Nations, thousands of delegates – overwhelmingly from governments and international organizations – descended on Dubai in the United Arab Emirates (UAE) for two weeks of WCIT. Their intended goal was to discuss a comprehensive update of the International Telecommunication Regulations (ITRs). These ITRs, which regulate such things as how telephone conversations are internationally connected and billed, had not been updated since 1988. Some proponents (including within the ITU itself) thought that something rather glaring was missing from these regulations: namely, the Internet. In a dramatic summit battle, these forces attempted to impose government control over the worldwide Internet, but were beaten back by Internet-freedom advocates, led by the United States. "Disaster averted," trumpeted a well-known forum for Internet freedoms following the rejection of the new ITRs by the liberal democracies. "No One Mourns the WCIT," read a headline on Forbes.com.

Thus, at least, goes a popular media assessment of WCIT. In fact, WCIT may not have been the clear victory for Internet freedom that it has commonly been made out to be. There was never a real chance that the United Nations would directly "take over the Internet," as some observers had breathlessly reported. However, it was always a real threat that WCIT would be used to further advance the interests of the authoritarian-minded states, who have been pushing for more state control over the Internet – a move increasingly resisted by liberal democracies. This could be accomplished by entrenching topics and especially terminology in a major international document – in this case, the ITRs – and leveraging that terminology in future diplomatic discussions. If this, indeed, was the plan, then it may have worked – and the target may have been the bedrock of the free Internet: the "multistakeholder approach" to managing the Internet.

Since its founding, the Internet has been managed through a bottom-up process generally known as the multistakeholder approach, which has been defined as the equal participation of governments, the private sector and civil society. In fact, the true order of importance in running the Internet is probably reversed: civil society has largely been responsible for much of the programming and protocols that form the nervous system of the Internet, while the private sector has provided the backbone. Governments have a fairly limited role to play. The Internet Corporation for Assigned Names and Numbers (ICANN), a U.S.-based but internationally minded non-profit organization, plays a more important role in the day-to-day managing of the Internet than any government organization.

In recent years, some governments have been trying to make up for this "historic accident," and have increasingly been asserting their right to be involved in managing the Internet. Some multistakeholder countries (such as the United States and virtually all of Europe) are more comfortable with the status quo, and argue that it is both practically and morally unsound to attempt to subordinate the Internet to governmental control. Other "cybersovereignty"-orientated countries (such as Russia and China) claim that the current order directly imperils their national security, primarily by denying these governments easy ways to control the Internet content consumed or produced by their respective populations. These countries demand that only national governments should have the right to decide about activity occurring in what they call their "national Internet segments." Most countries fall in between the two camps, with a sizable segment of the developing world harboring the distinct impression that the Internet boom is just a new form of imperialism, with most of the benefits of cyberspace accruing to large Western firms.

Before Dubai, all three of these camps had only a few countries clearly associated with them. After Dubai, only a binary world seemed to be left – most of the developing world (minus India) had sided with the cybersovereignty advocates. WCIT had morphed into a battle that, effectively, resulted in the West against the rest.

WCIT was the perfect battlefield for the cybersovereignty advocates. At WCIT, this group pushed hard to extend the ITU mandate to include Internet governance, and sought to introduce language that would facilitate government interference with Internet content. In two weeks of high-stakes intrigue and conference maneuvering, two developments cast a particularly bad light on the President of the ITU, Hamadoun Touré, and the UAE chairmanship. Firstly, despite U.S. resistance, delegates voted on controversial modifications to Article 5 of the ITRs. This article, which on the surface addressed important issues for the developing world related to SMS (text messaging) services, also addressed spam and therefore – indirectly – Internet content. Secondly, in a bizarre "no-vote" at 1:30 a.m. on December 12, delegates found out that, to their surprise, they had been apparently tricked into voting on the controversial (if non-binding) "Internet Resolution," which was subsequently included in the appendix of the ITRs. For some delegates, this already meant that WCIT had breached a taboo by trying to include Internet issues within the ITU agenda, a trend that continued to the final day of the conference. On that day a cunningly exploited opportunity allowed the Iranian delegate to use a discussion on human rights to force the issue of state rights to access international telecommunication services (including the Internet) into the preamble. This move, an apparent attempt to conflate state rights with human rights, was the last straw. In the end, 89 countries, including Russia, China, Saudi Arabia and Singapore, signed the new ITRs on the spot, while 55 countries, including the United States and nearly all of the liberal democracies, did not. By voting, the ITU broke the

After Dubai, only a binary world seemed to be left - most of the developing world (minus India) had sided with the cybersovereignty advocates. WCIT had morphed into a battle that, effectively, resulted in the West against the rest.

tradition of "adopting by consensus" and thus ensured that the new ITRs would not be universally implemented. WCIT, therefore, was a failure."

However, the definition of "failure" may well be relative. In fact, WCIT may have primarily been a setback for the multistakeholder nations, and a victory for the cybersovereignty advocates. Similar to what happened at Yalta in 1945, the United States and like-minded nations may have made two significant mistakes – ignoring facts on the ground but also tolerating ambiguity in critical definitions. The first error means that additional countries will probably sign up to the ITRs. The second error explains why it could be a disaster if they do so. While the ITRs themselves are not really a direct threat, the wider implications of the language used in the document could well be a "semantic beachhead" with which to further attack the issue of multistakeholderism in Internet governance.

The most significant "ground truth" is that the vast majority of governments in fact agree with the ITRs, and may eventually sign them. While the ITRs have little direct impact on anything amounting to "managing the Internet," the threat is considerably more subtle. In any case, most countries would agree with at least some aspects of the cybersovereignty argument: namely, that as with traditional telecommunications or broadcast media, national sovereignty does at least somewhat apply in cyberspace. Despite what was said at Dubai, most governments support increased state involvement in the Internet. Even liberal democracies quite comprehensively manage "their" Internet space already. While most of the regulation is discreetly kept in reserve for emergencies – or safely hidden within the remit of the intelligence services – most liberal democracies also constantly manage their Internet space for "bad" Internet content such as cybercrime. Yet multistakeholder countries are very concerned that the cybersovereignty countries will justify increasing state control of the Internet through arguments about cybersecurity and cybercrime, when the cybercrime those countries are most concerned with are "thought crimes" – i.e., anything amounting to political dissent. The fear of inadvertently supporting measures to suppress free speech is one of the primary stumbling blocks for those multistakeholder nations that actually do believe that the Internet needs to have more government involvement than it currently does.

But there are other stumbling blocks as well. There are major concerns among liberal democracies that internationalizing Internet governance could have significant security repercussions. For instance, until relatively recently most member states of the European Union, to say nothing of the European Commission, had firmly backed replacing ICANN with some sort of intergovernmental organization. This position radically changed in March 2010 when the former CEO

of ICANN, Rod Beckstrom, called attention to what he called the threat of cyberattacks on the very backbone of the Internet. A spate of Internet "spoofing" attacks from 2009 to 2010, in which large chunks of Internet traffic were suddenly rerouted through China, raised the specter of worse to occur if indeed an international organization was granted the ability to control worldwide Internet routing. Their common assessment seemed to be "better the devil you know," and thus they continued to support ICANN.

The two factors mentioned above – the fear of encouraging political suppression, and the uncertainty involved in handing over control of Internet resources to an intergovernmental organization – are probably the only ones preventing most democratic governments from agreeing wholeheartedly with the cybersovereignty argument. Indeed, in the next few years, it is absolutely possible that nearly all countries in the world, except for the United States, Canada and the European Union members, will sign the new ITRs. This would be a significant setback for the multistakeholder movement, and leads to the second, Yalta-esque mistake made in Dubai: tolerating ambiguity in definitions where there should be none.

The most dangerous part of the ITRs may not be, as widely reported in the Western media, Article 5 with its possible implications for Internet content. Instead, the real peril may lurk in the Internet resolution, which has been included in the appendix to the ITRs. While legally non-binding and therefore irrelevant for the ITRs themselves, the resolution is still part of the ITR package and has a certain standard-setting function. The danger is that the ambiguous language used in the resolution could lead to a fundamental reinterpretation of what Internet governance is internationally understood to be, with dire consequences for the freedom of the Internet.

Those nations that do sign up to the ITRs may well be agreeing to a "Trojan horse" that greatly furthers the ambitions of the cybersovereignty bloc. According to noted Internet governance scholar Wolfgang Kleinwächter, the language in the new ITRs could actually imply the creation of a "new" multistakeholder system for Internet governance, one that ultimately replaces the existing system with something working under the aegis and ultimate control of the ITU. This would mean that the equal balance of governments, private sector and civil society that, at least in theory, was the hallmark of the multistakeholder approach may instead be replaced by a model in which the state is paramount. Civil society and the private sector – the true heavyweight actors in the Internet – would instead be relegated to an "advisory" status, literally surrendering their right to build protocols and hardware as they see fit.

A series of upcoming international meetings will indicate whether there really is a hidden agenda to legally redefine the multistakeholder approach. A first test will occur at the World Telecommunications Policy Forum (WTPF), an ITU-affiliated meeting, to be held in Geneva in May 2013. If the WTPF does indicate that there is a movement aimed at redefining Internet governance, then the next great battle will be the ITU Plenipotentiary Conference in Busan, South Korea, in 2014. The Plenipotentiary Conference represents the most senior meeting of the ITU as a whole, and the Internet-related future of the organization could well be decided there once and for all. There even have been predications that, due to internal maneuvering, the ITU will not have a single European director by the time of the Busan conference, and therefore the multistakeholder countries will have no voice at all within the organization. According to this line of thinking, the ultimate aim of the cybersovereignty advocates would be the 2015 U.N. summit meeting on the Internet, the World Summit of the Information Society (WSIS). At the previous meeting in 2005, WSIS was instrumental in providing the presently-accepted definition of the multistakeholder approach. The 2015 WSIS meeting would therefore be the place to lock in any new definition of what the multistakeholder approach actually means.

If the cybersovereignty advocates produce enough momentum to change the specific definitions of both "multistakeholder" and "Internet governance" and lock in these changes at WSIS 2015, then the U.N. itself will have delegitimized the current multistakeholder approach.

The stakes are dizzyingly high: If the cybersovereignty advocates produce enough momentum to change the specific definitions of both "multistakeholder" and "Internet governance" and lock in these changes at WSIS 2015, then the U.N. itself will have delegitimized the current multistakeholder approach. Liberal democratic governments will then face a stark choice: they can surrender ICANN and hand over chunks of the global Internet functionality to an international organization (the ITU, most likely), or they can ignore the U.N. and support the existing system of Internet governance, and severely delegitimize the entire international system of peace and security in the process. Finally, it could come to what a Russian delegate at Dubai warned Reuters of: "maybe in the future we could come to a fragmented Internet." Indeed, at a cyber norm

workshop held at the Massachusetts Institute of Technology in September 2012, some observers claimed that a fragmentation of the Internet into a number of nationally-controlled internets was "inevitable," and already happening. For most liberally-minded people, all three of these futures are pretty bleak.

The only hope for liberal democracies may well be to go on the offensive: Rather than allow the multistakeholder approach to be increasingly squeezed into the field of Internet governance alone, the principle should be extended to other fields and not only limited to cyberspace. The field of human rights offers some interesting possibilities here. For instance, one option would be to push for the U.N. International Covenant on Civil and Political Rights (ICCPR) to be applied to the Internet as a whole. This would instantly upgrade the importance of the Human Rights Committee, now a largely ignored body of 18 non-state experts (elected by the U.N. General Assembly) that reviews U.N. members' compliance with the ICCPR. Empowering the Human Rights Committee in this way would also give credence to the multistakeholder approach. Even if it means a reappraisal of what exactly the multistakeholder approach means, this may well prove the smallest of all possible sacrifices.

The alternatives are indeed dreadful: A world in which the global Internet is put under strong governmental control, or a world in which not only the Internet is fragmented by digital "iron curtains" but the entire international system of security is discredited with it. In such a world, we might truly look back at Dubai as the Internet Yalta, and wonder what might have been done differently.

Alexander Klimburg is a Fellow and Senior Adviser at the Austrian Institute for International Affairs.

About the Center for a New American Security

Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. The views expressed in this report are those of the authors and do not represent the official policy or position of the Department of Defense or the U.S. government.

Center for a New American Security
1301 Pennsylvania Avenue, NW, Suite 403
Washington, DC 20004

TEL 202.457.9400
FAX 202.457.9401
EMAIL info@cnas.org
www.cnas.org