Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms

James Andrew Lewis
February 2014

Europe and the United States have a collective interest in the promotion of a stable international order based on the rule of law, open and equitable arrangements for trade, and a commitment to democratic government and individual rights. These interests face renewed challenges in a complex global political environment.

Cybersecurity is among the most salient of these challenges. The fundamental issues in cybersecurity are to protect information (both intellectual property and personal information) and reduce the danger of disruption in the cyber environment and the critical infrastructures that depend upon it without damage to human rights or innovation. While many nations understand the risks they face in cyberspace, significant political differences create obstacles to collective action. Cybersecurity requires international cooperation to make the cyber environment stable and more secure. This essay's premise is that given their close and shared political and cultural values, Europe and the United States can work together to shape this foundation to reinforce both security and democratic values.

Did Snowden Derail Transatlantic Cooperation?

Until the National Security Agency (NSA) revelations, the United States and European countries had worked closely together to define responsible state behavior in cyberspace. The revelations about NSA intelligence activities created turmoil and affected the pace and scope of cooperation in cybersecurity. The leaks highlighted that the global networks we have come to depend upon are inherently vulnerable. Cybersecurity requires agreement among states, but the foundation for agreement is trust, and this has sustained damage.

Reaction to the leaks differs among member states. German reaction to the revelations has been pronounced and Berlin may demand more attention to the protection of citizen data as a part of future cooperation in cybersecurity. Differing competencies and competing political and commercial interests complicate the rebuilding of transatlantic trust. Transatlantic disputes over strategy are not unknown, particularly when European domestic politics and U.S. national security policy clash, but different political circumstances make these disagreements more perilous and perhaps more damaging.

Democratic norms are still relatively fragile—less fragile than in the past, but still not beyond challenge. It would be unfortunate if internecine disputes among the democracies had the effect of weakening the global defense of human rights or inadvertently bolstered the efforts of authoritarian regimes to restrict freedom in cyberspace. European nations have legitimate complaints about espionage, but if carried too far, there is a real risk to European and U.S. security that seems underappreciated. The core of transatlantic security rests on building an international system based on the rule of law, peaceful resolution of disputes, and respect for human rights. Europe and the United States learned this lesson painfully in 1939 and had it reinforced during the Cold War.

A serious effort to remediate the political effect of the leaks would embed remedies in a larger

1616 RHODE ISLAND AVENUE NW
WASHINGTON, DC 20036
TEL. (202) 887.0200
FAX (202) 775.3199

framework of cyberspace norms for governance and security. Transparent Internet governance, clear expectations about behavior, and better cybersecurity are the ingredients of post-Snowden transatlantic cooperation. Both sides of the transatlantic partnership need to take action to achieve this. The United States will need to bring its espionage practices in line with the expectations of its allies and demonstrate political commitments on restraint and privacy commensurate with European expectations. This will require steps by the United States to reassure European partners, address the concerns of the European public, and establish new ways to work with the European Commission within its trade and law enforcement competencies. In turn, the commission and member states need to define the scope of reciprocal action that they can take and how best any new cooperation can advance both transatlantic security and global human rights.

From Transatlantic to Global: The Politics of International Cybersecurity

Even without the leaks, we would need to reassess cybersecurity. Powerful myths shaped our understanding of cyberspace, but they no longer reflect its political realities. The view of the Internet pioneers, largely from the U.S. technical community, was that cyberspace was a borderless commons where civil society could assume many of the traditional functions of governments.[1] These views reflected commonly held views on the future of international relations from the 1990s. The end of the Cold War, and the incorporation of communist states (particularly Russia and China) into the Western "system" of state relations and institutions, seemed to herald an end to conflict and a decline in the importance (or perhaps utility) of nation-states and Westphalian sovereignty.

In retrospect, these assumptions were wrong. Governments suffered a temporary decline in influence until they could adjust to the Internet and its political, security, and economic effects. Nation-states are still the most powerful actors internationally and we are seeing the steady, incremental expansion of sovereign control into cyberspace as governments attempt to manage risk and obtain advantage from digital networks.

The greatest challenge for the civil society model is in international security. The nonstate approach depended on implicit understandings and voluntary private action to secure cyberspace, which proved inadequate in the face of determined and largely untrammeled state actors. Nations were quick to exploit for intelligence purposes a global network built with inherently unsecurable technologies. The speed and scope of connectivity led to a flourishing of espionage and transborder crime, often state-sponsored, that overwhelmed a governance structure designed for commerce.

Any effort to change this comes at a moment of global political transition. Powerful non-Western economies are expanding their regional leadership and international influence. While the form of international governance is "Western" and derived from the European diplomatic tradition, many new participants do not share the common experiences and culture that underpin the transatlantic relationship. Colonialism shapes these nations' historical experience more than global war to defend democracy. Economic decline in Europe and Japan, combined with serious missteps by the United States, have reduced the influence of the Western democracies at a time when new entrants are asserting themselves in international issues.

Non-Western states with different cultural background and different historical experiences ask why they should accept unquestioningly the institutions and agreements put in place at the end of the 1940s, when a much smaller and largely transatlantic community dominated

[1] Here, "civil society" is composed of Western nongovernmental organizations and Western corporations.

world affairs. Nor did Cold War success mean that Russia and China agreed to docilely follow Western rules. Other countries share this discomfort with rules developed when most were not yet independent.

The different historical experience of the new entrants leads them to take a conservative approach to international relations where respect for sovereignty makes them reluctant to intervene in other nations. There is also reactive element impelled by discomfort with the unipolar moment and the excesses of the U.S. war on terror. These factors create a degree of alignment with the authoritarian regimes that are also challenging Western norms and institutions, albeit for different reasons.

As influence and power have diffused throughout the globe, non-Western nations question the institutions and agreements shaped during the period of Western dominance. The legitimacy of these institutions has been frayed and must be repaired. There is pressure from the new entrants for reconsideration and rebalancing to reflect their differing interests and their growing influence. A rebalancing of international power is inevitable given the growing importance of these countries, but the form this rebalancing will take remains open and still undefined.

One of the successes of the Universal Declaration of Human rights (UDHR) is that it established basic freedoms as global norms. Citizens in countries around the world expect to exercise these rights, including the right of untrammeled access to information. Most of these new powers, including influential nations like India, Brazil, and South Africa, share the transatlantic commitment to democracy and human rights, and in particular the right of free speech. These expectations create political pressures and shape government attitudes in ways favorable for reaching global agreements on cybersecurity that reinforce democratic norms. The commitment of most new powers to freedom of speech is a significant difference with the authoritarian regimes and their plans for cyberspace.

The Status Cybersecurity Diplomacy

A loosely coordinated Western diplomatic strategy to define norms of responsible state behavior has guided transatlantic efforts in international cybersecurity to date. Two developments—the challenge to U.S.-centric Internet governance seen at the World Conference on International Telecommunications (WCIT), and the NSA leaks—have put this coordination under pressure. Two other developments—progress in the UN Groups of Governmental Experts (GGE) and the Organization for Security and Cooperation in Europe (OSCE) on norms and confidence-building measures—show where the strategy has worked.

WCIT struggled with alternate visions for the Internet's future. This was not a bipolar contest, with the West automatically on the side of righteousness. Governments as diverse as Malaysia, Vietnam, and India want their values and national laws to have precedence on their national networks. Economic considerations swayed many countries against the incumbent structure. Russia and China argued persuasively that this global resource should be managed by all nations, under the auspices of the United Nations. The largest single bloc, 87 nations, led by regional groups from the Middle East and Africa, supported Russia and China's proposals for a greater government control of the Internet. The second-largest bloc was undecided. Only a minority supported the Western position, in part because others saw it as a defense of the legacy structure.

WCIT highlighted the convergence of security and governance, but it also highlighted the obstacles to meaningful treaty commitments. Norms remain the best approach because there is too much distrust among competing nations for any legally binding agreement. Cyber treaties face major problems over compliance, agreement on terms, and, fundamentally, deep

suspicions that the "other side" would cheat. No single treaty could embrace the full range of cyberspace issues and a treaty negotiation would likely become an effort to rewrite and diminish existing agreements on trade, human rights, or law enforcement. A rough hierarchy for international agreement on cybersecurity would begin with confidence-building measures to create trust, using this increased trust to reinforce norms of behavior, and eventually and if necessary, transforming these norms into binding international agreements.

Unlike a treaty, norms are not legally binding. They reflect instead expectations about behavior. A normative approach to cybersecurity draws upon the experience of nonproliferation. With the Missile Technology Control Regime (MTCR), for example, a few like-minded Western nations agreed that responsible states do not transfer ballistic missile technology. Over time, the number of adherent nations grew and there was acceptance of a new global norm of behavior. Agreements on controlling chemical and biological weapons followed a similar pattern, with institutions like the Australia Group providing a mechanism for like-minded nations to cooperate. A similar approach to cybersecurity offers the greatest likelihood of increasing stability and security in cyberspace.

We can dismiss the argument that norms are too weak, given their success in shaping other areas of international activity and because there is no serious alternative. Our experience with the problems of cybersecurity is too limited to guide binding agreement. Nations will ignore cyber treaties that are unenforceable. For the foreseeable future, treaties face fatal implementation problems involving scope, compliance, and verification. Norms for responsible state behavior in cyberspace should remain the centerpiece of a revised transatlantic strategy.

The work to build confidence and define norms has been a multifaceted effort to define state responsibilities toward other states and their citizens, with efforts in the United Nations, regional groups, the "London Process,"[2] and the Budapest Convention on Cybercrime. While there are regional differences (certainly in pace, if not substance), there is an emerging consensus about responsible state behavior in cyberspace. The issue now is to further develop cyber norms, win greater acceptance for them, and identify when norms must be modified or created for cyberspace.

Defining norms will be a difficult task for the international community, given disparate views on rights, sovereignty, and control. Russia (which tabled a cyber treaty in the United Nations as early as 1998) called in 2003 for the United Nations to create a Group of Government Experts (GGE) report on possible areas of cooperation to reduce political and military risk in the new digital environment. The first GGE produced a lengthy draft report to which no one could agree. The second GGE (2010) produced a very short text recommending that the international community further develop norms and confidence-building measures (CBMs) and build capacity in developing countries.

Any diplomatic strategy will need to change in light of the NSA revelations and their effect on U.S. influence, but not as much as an initial appraisal might suggest. The United States can no longer be solely the demandeur in discussions of cybersecurity, but fundamental transatlantic interests for greater stability and security in cyberspace have not changed as a result of the leaks, nor has the shared commitment to democracy. The 2013 GGE and the OSCE CBMs provide the foundation for further progress.

[2] The London Process, launched by UK Foreign Secretary William Hague, is a series of information international meetings whose aim is to generate a consensus on responsible behavior in cyberspace. Initially the London Process was seen as the vehicle for gathering like-minded nations to agree on norms, but its goals have become more diffuse.

The June 2013 Report of the UN Group of Governmental Experts produced agreement among countries as diverse as the major NATO allies, Russia, India, and (reluctantly) China. This agreement, later endorsed by the secretary general and the General Assembly, has reoriented the political landscape for the discussion of cybersecurity. The GGE's foundational element is affirmation that existing internal commitments apply equally in cyberspace as they do in the physical domain.[3] The GGE set important precedents that will guide future discussion of international cybersecurity. The Organization for Security Cooperation in Europe (OSCE) work on CBMs to increase transparency and coordination among OSCE members[4] complements the GGE norms. The OSCE's CBMs are also a useful precedent. The adoption of similar CBMs in other regions will help build the trust required for more detailed norms and understandings.

Differing roles and responsibilities for international affairs between the European Commission and member states will also shape diplomatic strategy. Previously, the commission had taken a "homeland security" approach to cybersecurity, consistent with its economic and public-safety responsibilities, while the member states had responsibility for political-military issues. Consistent with the 2013 EU cybersecurity strategy, the European External Action Service can play a role in advocating norms for international behavior as part of the European Commission's larger diplomatic engagement. The nonproliferation experience showed the importance of a joint effort where the United States, Japan, Australia, European nations (which have primary responsibility in Europe for security and defense issues), and the commission presented a consistent message on norms to persuade non-Western nations that nonproliferation was indeed a global norm.

Transatlantic cooperation could benefit by greater attention to the role of NATO. Agreement within NATO on thresholds and collective defense obligations would advance progress on norms. An expanded role for NATO in transatlantic cyber defense is politically unacceptable, but NATO members should develop common understandings on when a cyber incident moves from being a threatening, politically coercive action (as we saw in Estonia) to being use of force or its equivalent.

Member states have been reluctant to clarify responsibilities between NATO and the civil authorities in member states and the European Commission for determining action and response. Putting aside the troubling implications of fractured responsibilities for collective defense, NATO will inevitably face a decision about how to respond to some future cyber incident against its own networks or the networks of a member state. The context for a decision (or set of decisions) on responding to a cyber incident will be one of greater-than-usual ambiguity and uncertainty for the NATO's leaders. They would do well to discuss and perhaps practice potential response. Greater clarity for both member states and for an external audience and agreement on what type and level of malicious cyber activity could trigger Article V (collective defense) and what kind of messages or "signals" NATO would issue during a cyber crisis would increase stability in cyberspace and reinforce any larger transatlantic effort.

---

[3] These include the applicability of international law, and in particular the Charter of the United Nations, and the international norms and principles that flow from state sovereignty; respect for human rights and fundamental freedoms; cooperation against criminal or terrorist use of cyberspace; responsibility by states to meet international obligations regarding internationally wrongful acts attributable to them; and an appropriate role for the private sector and civil society

[4] Measures agreed in the OSCE include the voluntary provision of national views on doctrine, strategy, norms, threats, protective measures, and concepts of operating in cyberspace. OSCE member states will share information on national organizations, programs, or strategies for cybersecurity, identify contact points to facilitate communications and dialogue, and establish links between national Computer Emergency Response Teams (CERTs).

The Authoritarian Alternative for Cybersecurity

Regimes that fear access to information are using the demand for greater security to promote policies and rules that restrict openness. The limitations of the current multistakeholder model to secure the digital infrastructure provide an opportunity for authoritarian regimes to offer an alternative approach to governance and security. This alternative reflects differing concepts of sovereignty, stability, and security in cyberspace, reinforced by hostility to the West (and to U.S. preeminence). The basis of the competing model calls is global adoption of Russia and China's International Code of Conduct for Information Security and a leading role for the International Telecommunication Union (ITU) for cybersecurity and for governance.

First, the Code of Conduct is an ill-disguised effort to dilute the Universal Declaration of Human Rights. The UDHR creates norms for state behavior. States that violate these norms lose legitimacy in the eyes of both the community of nations and their own citizens. For Western nations, the long conflict with totalitarianism showed the central importance of human rights for international stability. The counterargument is that holding nations accountable is interference in the internal affairs of a sovereign state. In the 19th century, when human rights were not part of the international political agenda, this was accepted international practice. The Code attempts to reclaim some of the freedoms sovereigns lost in acceding to the UDHR. It reflects a larger debate on the interaction between sovereign authority and universal rights that the transatlantic community must take into account in developing a shared approach to cybersecurity.

Second, assigning the ITU a central role in cyberspace would likely lead to politicized or statist processes for managing cyberspace. This puts both innovation and access to information at risk. The current, "multistakeholder" model is properly criticized for being overly American, inadequately representative of the new users of the Internet and the states that represent them, and unable to deliver key public goods, such as security. The benefits of the multistakeholder model is that it allows for a much greater range of innovation in the use of cyberspace, lets markets rather than governments guide technology, and has been stunningly successful in creating and expanding interoperability and connectivity using privately developed standards and protocols. Giving the ITU these responsibilities would be a step away from privatization, and the ITU's capacities would be strained if it took on new tasks dealing with international security or crime.

A strong political imperative drives the authoritarian alternative. For democracies, the political effect of the Internet is changing the nature of electoral politics, but democracies are used to dealing with dissent and debate and have mechanisms to accommodate political challenges. Nondemocratic regimes are brittle, since they lack political mechanisms to accommodate dissent. The Internet and the profusion of information create risk (or the perception of risk) for these regimes. This is the primary reason Russia and China prefer to say "information security" and "information space," instead of cyberspace, which they regard as limited only to technology and not including content. The Internet creates significant political risk for them and they seek international agreement to reduce it.

The authoritarian alternative reflects an older concept of sovereignty and "non-interference with internal affairs"—the norm for state behavior before 1945, before democracies realized the importance for international security of rules on how countries would treat their own citizens.[5] The antagonism between this older concept of sovereignty (which gave each state

[5] Jack Donnelly, "State Sovereignty and Human Rights," *Human Rights and Human Welfare Working Papers* no. 21, June 23, 2004, http://www.du.edu/korbel/hrhw/workingpapers/2004/21-donnelly-2004.pdf.

unimpeded rights as to how it treated its citizens[6]) and the "universal" agreements on rights is a source of tension in international affairs and it shapes the discussion of cybersecurity. International human rights commitments are largely a Western creation, and nations that were not part of the West did not participate in their development and do not necessarily endorse their precepts. Many countries would prefer to limit access to some online content.

The asymmetry in political risk is one of the central complications for reaching international agreement on cybersecurity and an important consideration for negotiation, but it should not obscure the larger strategic goal of collective action in cyberspace. A transatlantic approach must balance the requirements for near-term agreement with nondemocratic states with the need to place global cybersecurity on a foundation of principles and norms that reflect democratic political and economic values. Multilateral discussion of cybersecurity among nations with disparate views of risk will involve defining the boundary for sovereign action and the limits of international commitments. This is an opportunity for transatlantic community if it can find flexible approaches that accommodate the concerns of new users while placing global cybersecurity on a foundation of principles and norms that reflect democratic political and economic values.

Information Age Norms

Any discussion of norms must go beyond traditional political-military concerns or simple endorsement of existing international law to ask what new norms are needed for cyberspace. The characteristics of the cyber environment that new norms must reflect are access to immense amounts of information and an enormous expansion of the "political space" (for discussion, debate, and association). Access to information now determines the relationship among states and between citizen and state. Access to information and the opportunity for a greater voice in public affairs shapes citizen expectations for how they will be governed and creates powerful centripetal forces that are remaking social and political systems.

The expanded role of information changes the requirements and expectations for political legitimacy. Legitimacy is the source of authority. Legitimacy is created by the consent of the governed, as they acknowledge authority and assent to its rules. A complex political tradition derived from the Enlightenment links legitimacy and assent, and assumes that the exercise of "reason" will lead a majority of citizens to assent to the best policies (in practice, of course, this may take many iterations and much debate). The Internet has changed the requirements for legitimacy and assent, and new norms must take into account citizen expectations about cyberspace and access to information.

A March 2010 survey of more than 27,000 adults in 26 countries found that 87 percent believed that complete access to information on the Internet should be a "fundamental right." This was true for countries rich and poor and as politically as diverse as Sweden and China.[7] Ensuring access to information is crucial for long-term stability in cyberspace because any agreement that does not guarantee access to information will face immense public resistance. Cybersecurity norms must establish expectations for state behavior on free access to information and the protection of personal information, intellectual property and human rights.

Access to information does not mean a complete absence of constraint. Countries have the right to create reasonable and minimal restrictions on certain kinds of information if these restrictions do not transgress their international commitments for human rights and for trade—restrictions on child pornography are a universal example of this. The optimal policy,

[6] Hence the frequent objections to "interference in internal affairs."
[7] BBC, "Internet access is 'a fundamental right,'" BBC.co.uk, March 8, 2010, http://news.bbc.co.uk/2/hi/8548190.stm.

however, must be to allow access to information rather than restrict it.

The Internet redefines legitimacy in international politics by increasing the need for persuasion and openness as tools of influence, and by requiring broader involvement by new participants—both governments and private actors—in diplomatic and governance processes. Cybersecurity norms require not only extending the current framework for interstate relations in trade, conflict, and human rights into cyberspace, it requires meeting the new obligations for transparency and access to information that are reshaping global expectations about legitimacy.

Only norms that take into account the central role of the right of access to information will produce security and stability. While identifying new norms will require debate and experimentation, agreement on norms is essential for building international governance structures and mechanisms for collective action to fit the new international political environment, and an opportunity for transatlantic cooperation and leadership.

A Transatlantic Framework for Responsible State Behavior

The starting point for international cooperation in cybersecurity is agreement on the applicability of existing international law and the existing norms of behavior that govern state relations. The path for extending the definition of responsible state behavior into cyberspace lies in agreement among states to observe their existing commitments in international law on human rights, trade, and armed conflict. While nations have taken initial steps in this direction, with agreement in the General Assembly that human rights apply equally in cyberspace and with the 2013 GGE, it is imperative to define an expanded set of norms for cyberspace.

New norms could include measures to ensure continuity, security, and stability of the Internet. They could also include measures to ensure an open, interoperable, reliable, and secure Internet, and a modernized and globalized multistakeholder approach to governance. Norms fall into five categories: international security, governance, political rights, development, and data protection.

- **International Security**

Concerns about the "militarization" of cyberspace or that international agreement on the applicability of the Laws of Armed Conflict (LOAC) will legitimize cyber conflict are specious. All major military powers have developed cyber attack capabilities. It will be more productive to clarify and expand constraints on the use of cyber attacks. The 2013 GGE affirmed that existing international laws governing armed conflict apply to cyberspace, but there are areas of ambiguity and opportunities for further development. International law calls for nations to exercise proportionality, distinction, and discrimination in the use of force. All three have areas of ambiguity. Pictet's criteria of scope, duration, and intensity are a starting point for assessing what is a proportional response to a cyber attack, but these decisions are left to national discretion. A discussion to increase common understandings on proportional responses to different classes of cyber attack would reduce risk.

Expanding the limits on collateral damage (unintended damage to noncombatants) is crucial because the risk of collateral damage is greater in the case of cyber attacks, given the higher degree of connectivity among networks. Physical distance from the target is not a barrier to damage. These factors increase the risk that a legitimate attack will have inadvertent consequences, making international agreement to limit the risk of collateral damage a foundational norm for cyber conflict.

LOAC currently forbids attacks on civilian targets unless there is some overriding military

necessity. Belligerents are expected to avoid attacks that cannot reasonably be limited to a specific military objective or which are indiscriminate or haphazard in their inclusion of civilian targets. This reflects the practical reality that combat knows few bounds. Civilian targets have been attacked in every war. However, there could be international agreement that some targets (core Internet infrastructures, such as the "root servers" of the Internet addressing system, nuclear power plants, or nuclear command and control networks), where the risks of collateral damage (and conflict escalation) are so great that any attack should generally be avoided.

Norms could also stigmatize certain cyber weapons, as the international community has done with classes of weapons of mass destruction (WMD). WMD is stigmatized because of the weapons' demonstrably horrific effect; cyber attacks, outside of science fiction, do not produce the same damage. It is also difficult to define a cyber weapon, given the range of techniques available for creating them and the widespread availability of software. A starting point could be transatlantic agreement that nations will not transfer or allow the transfer of cyber tools specifically designed to damage critical national infrastructure, Stuxnet being a primary example.

- **Governance**

The existing Internet governance needs to change to meet citizen expectations. A sustainable and legitimate structure will need transparent and accountable processes for an expanded community of Internet users. A new approach to governance must be based on democratic political and free-market norms if it is to be sustainable

The emergence of a global Internet community and the vastly increased reliance on the Internet for crucial economic activities challenge the civil-society approach that lies at the center of the governance structure created by the United States in the late 1990s. This governance structure was created for a smaller Internet where most users were Western. It was based on rosy and comfortable assumptions about the future of international security that underestimated risk. Change in this legacy structure is inevitable but the form this change will take remains unclear.

Change does not mean a wholesale replacement of the existing governance structure, but modernizing it to reflect a global polity and new responsibilities. A likely path for change is consistent with a middle way for Internet governance, between those who reject any change and those who seek greater political control of the Internet. Neither governments nor the private sector are by themselves capable of managing this complex new global infrastructure. A transatlantic approach to governance should endorse concepts and that are least disruptive to global connectivity and to stable operations, and least constraining to trade, future growth, innovation, and human rights.

Clarifying the role of the United Nations is a key issue for global discussions of governance. Many new Internet user nations believe that Internet governance is best entrusted to formal governmental bodies anchored in the United Nations. A governance system not associated in some way with the UN system will not be perceived as fully legitimate by these new users. As these states assert a greater role over their national networks, there will be an almost tidal pull toward assigning the United Nations increased responsibilities. However, there is reasonable concern that changing a system that has worked so well as the Internet expanded to encompass billions of users for one that may be less flexible and more politicized will harm the global interest.

Cybersecurity and Internet governance cannot be treated as unrelated issues. The clearest overlap between governance and security involves the manipulation of the Internet

addressing system for political, espionage, or military purposes. At least one country has experimented with these techniques, either as a weapon to disrupt Internet services or to control political dissent. Existing governance structures find this difficult to prevent and agreement among states is the best way to reduce risk and increase stability.

New norms for governance could include commitments to ensure an open, interoperable, reliable, and secure Internet operated by the private sector, within the framework of existing government commitments on trade, crime, and security. They could emphasize that operational and technical aspects be left to existing nongovernmental groups like the Internet Engineering Task Force, similar to the approach taken in governing other global infrastructures, such as finance, air travel, or shipping, where responsibilities are divided between public- and private-sector actors. Finding the right balance between the state and private sector and modifying (or developing) the best institutional structure will be an iterative process that transatlantic agreement can help to shape and guide.

- **Political Rights**

The Internet is a barb in the side of authoritarian regimes. It provides their citizens with access to alternative (and usually more accurate) sources of news. It creates the ability to express dissent, organize, and coordinate political activities. Democratic societies incorporate dissent into their political processes and consider these actions to be routine. Authoritarian regimes do not have mechanisms for dealing with dissent other than coercion. The quandary for authoritarian countries is that they want the Internet to be open for business but closed for politics. They see free access to cyberspace as a source of political, military, and social risk, yet at the same time, they are drawn to the economic potential that cyberspace creates.

Authoritarian countries have put in place extensive national controls on access and use of the Internet. These national controls are inadequate. Services and information located outside their boundaries are still accessible to their publics. They seek to “internationalize” control through changes in Internet governance and in the standards and protocols, which reflect the democratic political values of their authors.

A central tenet of transatlantic cybersecurity norms must be that rights exercised in cyberspace deserve the same protection as those exercised in the physical world. Human rights are an essential component of international security. Beyond reaffirming the applicability of existing commitments to cyberspace, political rights need to be extended to take into account access to online data. The norm for state behavior must be to allow access to information rather than restrict it.

A transatlantic norm should extend existing rights so that they apply to services such as social networks, and ensure online access to information or services. In the framework of existing international law and practice, countries are free to create reasonable and minimal restrictions if these restrictions do not transgress their international human rights commitments, but there should be explicit recognition that fundamental freedoms of expression, assembly, and association apply equally to social networks. Similarly, a new norm could define responsible state behavior when it comes to protection of online identities (bearing in mind the “Digi-Notar” case where fraudulent certificates were used to identify activists to Iranian security forces), and for the protection of personal data located in social network servers or “clouds.”

- **Development**

Cybersecurity norms must include support for development. A credible approach to development is crucial for international agreement on cybersecurity. The World Conference

on International Telecommunications showed that development—access to broadband services to boost economic growth—is the most important consideration for emerging economies when they think about cybersecurity and Internet governance. A transatlantic effort could ensure that this broadband development is secure.

Cybersecurity capacity building must be "embedded" in a larger story of development and economic growth from increased broadband capabilities. It needs to avoid the pitfall of the existing narrative that links the Internet status quo to economic growth. Many non-Western governments, already tempted by the idea of sovereign control of informational resources, note that a lack of Internet freedom has not stopped China from outpacing Europe and the United States when it comes to economic growth. These nations have different attitudes to the relationship between government, business, and society. The "digital opportunity agenda" attempted to blend democratic values, development, and security into a lumpy and unpersuasive package. A better approach would assist developing countries in designing the policies and regulations that maximize broadband's contribution to growth while preserving essential freedoms.

There is overwhelming demand for mobile connectivity, and commercial network operators are best placed to build national networks in developing countries. Western experience shows, however, that cybersecurity will be an afterthought in the deployment of networks. This is one area where a coordinated transatlantic effort is vital. The United States and European nations can work with private companies and governments to make sure that broadband deployment is both secure and open—many nations have little or no cybersecurity capability, and providing training and technical assistance in building national cybersecurity capacity (training specialized law enforcement groups or strengthening national CERTs) can be done at relatively little expense.

- **Data Protection and Privacy**

The emphasis in cybersecurity has been the protection of intellectual property from cyber espionage. To this we must now add the protection of personal data. The central question is to define one nation's responsibilities regarding the data of another nation's citizens. A transatlantic norm could build upon strong domestic principles for oversight and accountability based on democratic principles and then press for their adoption internationally.[8]

It is in the economic interests of both Europe and the United States, given their dependence on intellectual-property-intensive industries, to strengthen compliance with existing IP protections and to develop additional measures for enforcing them. Concern over the consequences of irritating China has hobbled transatlantic action to resolve the problems, but weak IP protections cost Europe and the United States billions of euros in trade and thousands of jobs every year. While cyber conflict poses the greatest risk, weak IP protection is the most damaging cybersecurity problem. Changing this will require extending existing norms and perhaps creating new ones to protect data in cyberspace.

Enlightenment norms called for nations to recognize the equality of citizens and their right to freedom of speech, assembly, belief, and to seek redress for government action. To these the Universal Declaration of Human Rights, perhaps inspired by the horrors of collectivization and war, asserted the "security of the person," the rights of the individual and not just the citizen's rights as a political actor. The right to privacy is the foremost of the "post-Enlightenment" norms and redefines the relationship of the citizen to the state.

[8] This suggestion comes from Ronald Deibert, director of the Citizen Lab of the University of Toronto's Munk School of Global Affairs.

For privacy, the burden in the transatlantic relationship clearly lies on the United States. The recent U.S. commitment to extend existing privacy protections and to place limits on bulk collection of data on European citizens by government agencies is essential to rebuild trust. Additional steps might include reviewing the Safe Harbor Agreement or expanding protections for existing data-sharing programs, but this needs to be done in a way that does not hurt economic growth. Progress will also depend on how the United States and Europe agree on the implementation of new European Commission privacy regulations. These trade agreements will affect and shape transatlantic cybersecurity cooperation.

Pragmatic transatlantic understandings on the protection of personal data could create a global norm, but this will require that we recognize the lack of salience of privacy and the differing levels of concern in many non-Western governments for this issue. Given the opacity that most governments apply to their surveillance activities, agreement between the United States and Europe is the only path for greater protection of personal data on a global basis.

It will also require recognition of the need for reciprocity. Many Europeans want a right to seek "redress" from the United States when they believe their personal data has been compromised. In turn, European nations need to provide greater transparency into their own intelligence activities directed against U.S. persons and expand their public oversight processes for such activities. Reciprocity is essential: diplomatic experience shows clearly that unequal burdens are not sustainable.

Mechanisms for Transatlantic Cooperation

New structures could improve coordination in cybersecurity. An initial decision is whether to seek agreement among all states on norms and responsibilities in cyberspace or whether to move to building agreement among like-minded states (while leaving the door open for other nations to join at some later date). The two approaches are, of course, not mutually exclusive. An informal coalition of Western democracies, united by common concerns, has been effective in promoting agreement on international cybersecurity. The issue is whether this should become more formal, a group of like-minded nations that agree to norms and confidence-building measures. This was a path for success in developing global nonproliferation norms. The advantage of this approach is, in light of the revelations about NSA, that it will be easier to reach agreement on meaningful norms in a like-minded group than in an oppositional grouping. The disadvantage is that a transatlantic approach, unless carefully handled, may alienate non-Western democracies.

If there is not adequate progress in getting broad agreement on norms for international cybersecurity, the mechanism for building a normative framework can use agreements among transatlantic nations while continuing to push in global or regional forums for their broader adoption. The development of a like-minded process must aim to be inclusive from the start. This requires balancing the need for progress on identifying norms and the need to win broad support. The nature of any like-minded group remains to be determined. It could be as simple as a joint statement by nations on their responsibilities in cyberspace. The London Process (if it continues) or other existing groups, like the G-7 or G-20, lack the necessary "like-mindedness," and some new multistakeholder institutional structure for cybersecurity may be necessary in the future. Transatlantic agreement on a like-minded group must encourage later entry by nations not involved in its drafting.

Accelerating the pace of international agreement on cybersecurity requires a degree of boldness. Progress in dealing with other transnational problems, such as proliferation or money laundering, began with a small group of like-minded nations agreeing on certain principles and recommendations for cooperative action in dealing with the problems. Over

time, the small group was able to win broader support for the principles and gain additional members. The Financial Action Task Force, for example, began with 16 members (the G-7 member states, the European Commission, and 8 other countries). It now has 36 members and 8 observers. There has been reluctance in the past to move to a like-minded approach for cybersecurity because of the risk of alienating some countries, but the alternative is continued drift. Initial agreement on cybersecurity norms between the European Commission, the United States, and countries like Japan and Australia is the best approach to creating global norms.

Important nations like India, Brazil, and others share to a degree Russian and Chinese concerns over the transatlantic foundation of "universal" values, but they also share a commitment to free speech and democracy. This shared commitment offers a basis for partnership with the emerging powers if Europe and the United States can address economic, privacy, and sovereignty concerns in these nations. An effective diplomatic effort would see member states, the External Action Service, and the United States coordinate their efforts in approaching emerging powers to gain broad international support for responsible behavior in cyberspace.

A unified effort by Europe and the United States will be more persuasive than uncoordinated individual approaches. Transatlantic agreement will make it easier to deliver a consistent message to Russia and China on their responsibilities and the need to change their behavior. They will not wish to be cast as outsiders if other states agree on credible international norms. It could also potentially serve as the basis for multilateral agreement on institutions and on tangible consequences for irresponsible behavior in cyberspace.

Principles for Transatlantic Cooperation in Cybersecurity

Four trends shape the discussion of cybersecurity: the political effect of digital technologies, the emergence of newly powerful nations, the renewed challenge to democracy and human rights, and the global consensus to embed cybersecurity in the existing framework of state relations and international law and agreement. We can derive from these trends core principles to guide transatlantic action to make cyberspace more secure and stable. Principles that define an agreed vision for the future of cyberspace could guide transatlantic cooperation to create a normative framework and give weight and impetus to ideas that have emerged as central to the discussion of cybersecurity:

1. The commitments nations have made to each other apply equally in cyberspace.
2. Individuals are guaranteed the same rights in cyberspace that they have in the physical domain.
3. States' extension of sovereign authority into cyberspace must be consistent with all of their international commitments on the treatment of their citizens.
4. States bear primary responsibility for security, safety, and enforcement in cyberspace. Private actors and markets bear primary responsibility for technology, operations, and commerce.
5. National laws and international agreements should increase rather than constrain the potential of cyberspace for innovation and experimentation in the commercial, political, and social fields.
6. Nations will treat cyberspace as a central vehicle to promote global economic development and growth, with particular emphasis on the developing world.
7. Agreements on institutions and rules for cyberspace must be representative and created on the basis of reciprocity, accountability, and equality in representation.

8. State actions in cyberspace should not threaten the stability of this shared global resource and avoid incidental or unintended damage to critical information infrastructures.

These principles reflect the larger trend of the "normalization" of cyberspace as an integral part of the political fabric rather than something sui generis. They focus on state action for a number of reasons. Debates over the demise of the Westphalian state misrepresent the problem we face in cyberspace. The relationship between the state and its citizens and with other states is changing in light of the new informational tools, but nation-states remain the most powerful international actors.

These principles focus on nation-state actions, because states are the actors that citizens will most likely perceive as legitimate. States bear direct responsibility for the provision of public goods and political order, and they retain their dominance in the use of armed force. State actors pose the greatest threat to the security of cyberspace, particularly if we consider those states that offer de facto sanctuaries to cyber criminals or that have covert military programs. A voluntary compact among private actors, while helpful, will not constrain those states where the private sector plays a subsidiary role. Agreement among states is the focal point for adoption of norms of behavior and mechanisms for collective action in cyberspace.

Principles should create the basis for legitimacy of action and for greater international stability. The traditional U.S.-centric approach to collective action in cyberspace minimized the role of governments, but this will need to change as non-Western audiences with differing views of governance gain more influence. Finding a way to expand the governmental role without losing the benefits of private action is a central problem for cybersecurity, but agreement among states will lay the foundation for action by private actors. A joint EU-U.S. statement on the principles could guide international cooperation in cybersecurity and set a precedent for global cooperation.

Liberty, Equality, Connectivity

The debate over cybersecurity is an inflection point for the future of international relations. How the new global infrastructure is governed and secured will help determine if the future is more democratic and peaceful or riven by conflict. Europe and the United States know better than most the importance of democracy and human rights for international stability. Transatlantic countries share political values that emphasize the rule of law, democratic governance, free markets, and respect for individual liberties. These values are reflected in cyberspace as it now exists (given its Western origins), but they are not institutionalized in any meaningful way. An informal approach is no longer adequate in the face of global political challenges. The goal of transatlantic cooperation on norms for cybersecurity is to build the framework of agreements that will institutionalize these values in a secure and stable environment.

The existing "state of nature" in cyberspace is too Hobbesian to be sustained, as the Internet and the other digital networks that comprise cyberspace become the essential global infrastructures. A coordinated effort has the best chance to shape cyberspace's new political environment in positive ways. Transatlantic cooperation is crucial for cyberspace's evolution to continue on a democratic path. The mechanisms for this cooperation will vary, depending on the issue and shaped by the division of competencies among European nations, the European Commission, and NATO.

Nations are gradually extending control of their national networks, but these national solutions do not have extraterritorial effect. Assertive new powers will attempt to reshape the international agenda to use international agreement on cybersecurity and Internet

governance to address political issues created by access to information. There are legitimate reasons for governments to want a greater and more directive role in cyberspace, but there are real risks that expanded roles for governments will, intentionally or inadvertently, damage the rights and opportunities cyberspace now provides. A cooperative transatlantic approach could identify a path for progress in cybersecurity that can guide the extension of sovereignty, the transformation of governance, and the desire for greater stability. Any strategy will require different approaches for different audiences—authoritarian states, emerging powers, and the developing world—but the common core should be principles that reflect the shared transatlantic values.

A consensus on responsible behavior in cyberspace by states is emerging from the many discussions taking place round the world. This consensus is grounded in common views among nations on the applicability of sovereignty and international law, but it is preliminary, in need of further development and not locked in by any institution or agreed statement. Absent dynamic leadership, further improvements in cybersecurity will be slow, and a positive outcome not guaranteed. In this changing political environment, both Europe and the United States have an opportunity to advance fundamental transatlantic interests in the rule of law, open and equitable arrangements for trade, and commitments to democratic government and human rights.

James Andrew Lewis is a senior fellow and director of the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C., where he writes on technology, security, and the international economy.