Cybersecurity in Asia and the Role of U.S. Leadership

An Interview with James Lewis

The Internet has emerged as a platform for social, economic, and even military interaction. As these interactions grow in number and consequence, states are grappling with how to translate policy intended for the physical world into the cyber domain. The Journal sat down with cyber expert James Lewis of the Center for Strategic and International Studies (CSIS) to discuss how the Obama administration approaches issues such as Internet sovereignty, multilateral cooperation, and governance in cyberspace. Additionally, Dr. Lewis provided insight into how the United States and China are currently managing their relationship as well as how recent events, such as the North Korean hacking of Sony Pictures Entertainment, fit into global trends.

Journal: What are the most pressing challenges related to cyber security that the United States currently faces? For example, what are the impacts of cybercrime and cyber espionage on U.S. economic interests and national security? Given these challenges, how prominent is cyber security in the Obama administration’s agenda?

Lewis: One of the interesting things about a recent event CSIS held on cyber issues is that White House Cyber Coordinator Michael Daniel said, both publicly and in private, that the President takes a personal interest in this issue, so that is really great. And the administration has made a lot of progress in putting the pieces together for a more secure network environment for the United States. But, this environment is still by no means totally secure. It is easy to overestimate the losses, but cyber espionage clearly has some effect on competitiveness. It has an effect on competitiveness. It has an effect on international relations and the international community. There is a risk of attack on the United States—outside of crime or espionage—that could be disruptive. Overall, we have done an immense amount of work in the last seven years, but there is still a huge amount of risk.
For example, the Obama administration laid out the doctrine and the chain of command for the military use of cyber tools, both offensively and defensively. That was in Presidential Policy Directive 20 (PPD-20). The Obama administration came out with an international strategy in 2011 that was largely on the right course, though it probably needs to be updated. They started an international process of trying to build norms and confidence-building measures with both the Chinese and the Russians, who are our most powerful state opponents, as well as multilaterally. They have had some success in the Organization for Security and Cooperation in Europe (OSCE), some success in the Association of Southeast Asian Nations (ASEAN), good progress with the Russians until Crimea happened, and good progress with the Chinese up until China adopted a new and more assertive Internet policy.

Crimea is actually the event that has had the most effect, (not Snowden or anything else), on cooperation with Russia and China. Crimea has knocked cybersecurity cooperation with these countries off the rails. We will see if that changes. For now, it has affected discussions between the United States and China because previously this was a three-way conversation with two of the participants agreeing with each other—Russia and the United States, which put the Chinese in an awkward spot. Now the Russians are not there anymore, which has empowered the Chinese to resist. Internet security, particularly domestic Internet security, is clearly a priority for Chinese President Xi Jinping. So, China is more assertive and faces less external pressure.

Journal: Looking forward to an upcoming benchmark, our second question concerns the transfer of stewardship of the Internet Corporation for Assigned Names and Numbers (ICANN), the organization at the center of the domain naming convention. In 2014, the United States committed to transferring stewardship of ICANN, which currently operates on a contract with the U.S. Department of Commerce, to a “global multi-stakeholder community.” What are the broader implications of this potential transfer? What are the main arguments for executing such a transfer? What concerns might cause a delay?

Lewis: It is a widely held foreign delusion that the Department of Commerce uses ICANN to control the Internet. And, there are just so many errors in that statement that you really wonder about the sanity of people who think it. I worked at Commerce for a couple of years, and it is not the center of American hegemony. So, the transition of ICANN is, in that sense, not important.

But, it is important for this reason: for about fifteen years, we had an environment where the United States dominated the Internet. It was our thing because we invented it. When we came up with our original policies, we really were not thinking of a global market. We were thinking of how this would play in the United States. We had expectations about how the world would evolve, and thought it would become a world of

peace where market democracies worked with each other under the rule of law. But, that turns out to have been wrong. We are now in a much more difficult environment in which you have new entrants (Brazil, India, China) saying, “Wait a minute, why do not we have a voice in this Internet thing?” These nations have said the same things about the Permanent 5 on the United Nations Security Council and similar types of institutions. These new entrants say, “Maybe this is a plot to preserve American hegemony. In any case, we need a bigger voice.”

And the United States is struggling to deal with those requests because we are constrained by our ideology. We still have a very 1990s ideology when it comes to the Internet—and that ideology no longer works. Yet, we do not have a new line. And all of these countries are becoming more assertive. China in particular has decided ever since Xi came to office that China will play a larger, more dynamic, and more directive role in the Internet. That is the challenge of the ICANN transition: how does the larger transition to a globally governed Internet work out? ICANN was never a real lever to control the Internet, but it is becoming a symbol of how control of the Internet will change. The United States is kind of stuck. We say we believe in democracy, but a majority of the voters do not live in the United States. We say we believe in self-determination, but that means other countries get to pick their own rules. So, are we kidding or not regarding self-determination? And the United States gets that question explicitly from countries like India, China, and Malaysia: “What is it? This is what you say, but what you do is something else. What is the truth—democracy or control?”

The Chinese have a monolithic approach to culture, and that puts them at a disadvantage in this debate. China’s other activities in the region put them at a disadvantage. And the Chinese do not have a very compelling story when it comes to what they want to do. That said, it has some appeal to these other countries that are now saying, “I do not want to do what the Americans want me to do, I want to do my own thing.” In that case, China is the place to go. A parallel there might be the Asia Infrastructure Investment Bank. People got tired of hearing the Americans tell them they could not have coal-fired or nuclear power plants, and the Chinese are not going to tell them that. The Internet is on the same path. We are seeing a challenge to the unipolar vision of the 1990s.

**Journal**: Continuing on the point of China’s role, we have a question about the Chinese notion of Internet sovereignty. China has recently floated an “Internet sovereignty” policy in different international fora, which refers to governments monopolizing control of cyber activities inside their borders. Is this a reaction to the American 1990s ideology? What are the main components of China’s “Internet sovereignty” policy and what priorities are driving this policy? If such a policy were to gain traction internationally, what would it mean for the future of the Internet?

**Lewis**: You had a very powerful Internet ideology that came out with the creation of the Internet, and that Internet ideology tracked closely with how people thought about foreign relations in the 1990s. It was one of the heydays of globalization, during which many believed there would be a world where governments would play a smaller role,
borders would be less important, private actors would take the place of the state in performing many functions, and there would be less interstate conflict. That was kind of the vision. *The End of History* is the book that captures this, but it turns out to have been completely wrong.2

What happened regarding the Internet is that people said, “The Americans invented the Internet and they tell us there are no borders, so that must be true.” Then after a few years, people figured out that there are borders in cyberspace. It is a physical construct. And, if there are borders, then they can enforce their national laws on their national networks. The issue now is the division between sovereignty and extraterritoriality. I had this discussion with a senior Malaysian official, who said to me, “In my country pornography and gambling are illegal, but I have to put up with them on my Internet because America controls the Internet. Why does American law override my national law?” And I said, “It does not. You can do whatever you want on your national networks, but you cannot extend that extraterritorially and you cannot violate your international commitments, particularly your commitments to the Universal Declaration of Human Rights.” And the United States is advocating Internet sovereignty, too. There is agreement in the United Nations upholding that national sovereignty applies to cyberspace.3

**Journal:** Do you foresee big changes in the cyber realm as this concept of sovereignty in cyberspace becomes more prominent? Would it change the Internet as we know it today?

**Lewis:** This is not clear. I do not think the Internet will fragment. Balkanization is one of these terms that the marketing department invented to defend incumbents. Nobody is going to Balkanize the Internet because the economic value is too great. But, figuring out how to extend sovereignty requires both new policies and new technology. The Russians are pretty far along on this with their System for Operative Investigative Activities (SORM) program, which is designed to extend Internet control. The Chinese and others are also looking at how to control the Internet for political purposes. So, we may be seeing a powerful counter to the idea that there are universal values that should govern everyone’s behavior. We see that in China and other countries. These countries believe these are not universal values, but rather Western values. I happen to think they are wrong. We know from good polling by the BBC and others that most of the world believes free access to information should be a fundamental human right. So, the most likely outcome is that we will see an Internet where national laws are more powerful and where governments play a larger role, but access to information will continue to drive public demand.

---

Interviews

Journal: How important is it to U.S. interests to identify the physical origin of cyber attacks? Does the United States possess tools, diplomatic or otherwise, to motivate other countries to take actions against cyber criminals operating within their boundaries?

Lewis: Attribution is an overstated problem. I think the 2014 North Korean hack of Sony Pictures Entertainment was useful in that it may have persuaded some commentators that they had overestimated the difficulty of attribution. And that attribution will become easier over time. I wonder what the world looks like when you do have attribution. In some ways, some things will not change because the problem is not attribution. The problem is that there are some countries that are politically opposed to the United States and refuse to cooperate in law enforcement because the people engaged in cybercrime and cyber espionage are either proxies of the state or state employees. The May 2014 indictments against the five People’s Liberation Army (PLA) officials is a classic example. We have the goods on these guys: we have their pictures, their home addresses, and their phone numbers. But they will never go to trial. The issue is not attribution. The issue is agreement to enforce laws. The central issue for cybersecurity is coming up with an international agreement on what responsible behavior by a state looks like. We do not have that yet.

Journal: Do you see potential mechanisms for forging international agreements on responsible behavior in cyberspace? Will it occur in a global forum such as through the United Nations Groups of Government of Experts on Information Security (UNGGE)? Or is this development more likely to occur at bilateral levels or be informed by state practice?

Lewis: It is unclear. Part of it is that the United States is still relatively allergic to the United Nations. Some people have proposed the International Telecommunications Union (ITU), but the ITU was until recently dominated by the Russians. There are not really other mechanisms. People have said that we may be able to use the OSCE, the Organization of American States (OAS), or the ASEAN Regional Forum (ARF). That might work, but we have not found the right approach to gain broad international agreement.

The Dutch are having a huge conference—it is the fourth global cyberspace conference. However, the three previous conferences have largely been busts. I expect the Hague Conference will do better, but we do not have a good mechanism for reaching an agreement yet. I do not know when that will change. I think that the logical place would be the United Nations, but there is a reluctance to say that.

---

4 The United Nations Groups of Government of Experts on Information Security is a “group of government experts” (GGE) from fifteen states tasked with studying existing and potential information security threats and possible cooperative measures.

5 The International Telecommunication Union is a UN agency responsible for issues concerning information and communication technologies.
Journal: The 2013 edition of China's The Science of Military Strategy outlines in its information warfare section the application of China's “whole nation” war doctrine to cyber operations. The document references mobilizing entities outside of the public sector, including private corporations or citizens, for “network warfare operations.” In March of this year, a code developer’s website (Github) was hit by cyber attack affecting traffic intended for Chinese search website Baidu. The attack specifically targeted pages with links to websites blocked in China. Does this imply that China is employing “whole nation” warfare? Should we expect sites that China views as disruptive to experience increased attacks? If not, what do you think “whole nation” warfare might look like?

Lewis: I thought “whole nation” was an effort by the PLA to claim dominance in this space. In other parts of the document, they say that the Ministry of State Security (MSS) and the Ministry of Public Security (MPS) should, in a cyber conflict, be subordinate to the PLA. I think they may have listed the Ministry of Industry and Information Technology (MIIT), too. I thought the “whole of nation” approach was an effort by them to say, “We are in charge.” I do not see the Github thing as being that different from how the Chinese normally operate. I had a Chinese diplomat tell me, “There is no such thing as the private sector.” For them, the private sector is a tool. This mentality happens to be consistent with the emphasis that President Xi has put on controlling the Internet to minimize its political effects within China. But, I think their recent attack was just a demonstration of what they consider to be another tool for defending the regime. They are not always good at calculating the damage it does to them globally. Suspicions arose regarding the Chinese government network’s administration, the China Internet Network Information Center (CNNIC), after the administration issued suspect “certificates” of the kind used to identify websites as legitimate, which could be used to trick Internet users. This may have been unintentional, but the effect is that the CNNIC has been compromised in the global market. They probably did not think about that. There is a little bit of a tendency to overestimate China’s power in this. I think in some ways they are separate issues. You have a PLA claim versus the traditional political action.

Journal: Do you think that the approach of using sanctions versus that of using indictments is more likely to deter this kind of attack?

Lewis: The model that some of us have been talking about for several years now is thinking about how approximate the methods that got China to change its behavior in proliferation. The parallel is not exact, but the general idea is the same: develop global norms; get like-minded nations to agree to them; and put in place penalties for bad behavior. We also have to engage the Chinese constantly to say that this effort is not just the Americans being crazy. The whole world believes this is inappropriate behavior. That strategy is, I think, the best one we have. The alternatives are insane. For example,

6 The Ministry of Industry and Information Technology of China is a state organization responsible for regulating electronic communication technology, not content.
Interviews

are are going to hack back? Do we really want to start a war with the PLA? That is a bad idea. Are we going to make our defenses better? That could possibly happen before the end of the century. So, in a diplomatic engagement strategy, sanctions, indictments, engagement, and winning international agreement on norms of behavior are all a part of the strategy.

Journal: Not only U.S. adversaries, but also many U.S. partners and other nations have started to raise cybersecurity issues on their national profiles. Have you seen any states, particularly in Asia, that you believe have made great strides in this area? Has the United States made strides in its cooperation with countries? What areas are ripe for cooperation, but remain underexplored at this point?

Lewis: The Republic of Korea, Japan, China, India, and Australia have all played a much larger role in thinking about the Internet. Vietnam and Malaysia have also played larger roles. A lot of Asian countries have engaged and a lot of them are thinking about the issues we have talked about. For example, how should cyberspace be governed? How can we make it stable? What would responsible state behavior look like? Furthermore, cyber is not a thing unto itself. Cyber fits into the larger context of international relations, so these countries consider this fact in their relations with China, their attitudes towards the United States, and their trade requirements. Cyber is an aspect of their larger foreign policy. And, in that sense, the one that is been interesting to me is—and this, of course, goes back decades—the lack of some kind of regional security framework in Northeast Asia. There is nothing like the OSCE, there is nothing like the OAS, and there is nothing like ASEAN. If the international community could get something like the Six-Party Talks on cybersecurity, that might be interesting. But it seems too difficult to do now. The Chinese say they will play, but only if the Americans are not in. The Russians do not want to play, and the North Koreans are crazy. It is just messy. Northeast Asia is one of the flashpoints for cyber conflict. It would be useful to have something like the OSCE. There have been a couple efforts and none have worked out, but I am not exactly sure why.

The Dutch are having a huge conference—it is the fourth global cyberspace conference. However, the three previous conferences have largely been busts. I expect the Hague Conference will do better, but we do not have a good mechanism for reaching an agreement yet. I do not know when that will change. I think that the logical place would be the United Nations, but there is a reluctance to say that.

Journal: Disputes about hacking, industrial espionage, and intellectual property violations seem to dominate narratives regarding the U.S.-China relationship as it pertains to cyber security. You have previously stated, “There is a risk that we could find ourselves in a conflict, given the deep problems between the United States and China and the worsening public perceptions on both sides.” Is there any room for cooperation on other cyber-related issues in order to change the tone of the U.S.-China cyberspace dialogue?
Lewis: No. We are at a very early stage in discussions with the Chinese. People think we would make more progress if we had a common lexicon, but the lexicon is not the issue. The issue is the fundamental differences between the two countries that are not only political in nature, but also have real military implications. It will take years of engagement to get to the point where we can approach something like the understandings we had with the Soviets before the end of the Cold War. The U.S. and Chinese positions are very far apart. Here is a good example: CSIS hosts discussions with Chinese scholars and Chinese officials. In the ninth and latest round of discussions, the Chinese participants said on day one that they wanted to cooperate. On day two, we had a tabletop exercise based on Sony. We said to them, “This is your chance to cooperate.” They replied, “We do not want to cooperate with you.” So, which is it? There is a general commitment to finding areas to cooperate, but when we get into the specifics there is nothing there.

I have another funny story in which there was an agreement between the United States and Russia to establish a hotline for cyber incidents. Putting aside the utility of a hotline, which is open to question, it is a nice gesture. There is a phone in the Kremlin and a phone in the State Department and you could pick them up and say, “Hey, what is going on.” And in an earlier round of discussions at CSIS, a Chinese representative noted that the United States and China already have a hotline between the PLA and the Department of Defense (DOD). The DOD representative said, “Yes, but you have told us you want forty-eight hours notice through diplomatic channels before we call you on the hotline.” Even the Chinese burst out laughing at that one.

The levels of distrust between the two governments are very high. If this were Chinese industry or China writ large, it would be much easier to find agreement because the differences between the two populations are not so great. However, because of the Chinese government’s limited access to information and its ideological controls, and given the fear that the anti-corruption campaign has created, the Chinese are not going to be doing any deals with the United States any time soon.

Journal: You mentioned the Sony incident earlier and we would love to talk about that a little bit more. In a recent article for 38 North, you argued that “the challenge of the Sony attacks is not persuading skeptical amateurs but signaling to North Korea and others the limits of covertness in cyberspace and what lines they should not cross.” What steps might the United States take to successfully signal where these limits lie? Do you think the Obama administration has been successful in setting these limits?

Lewis: There are three parts to the response to North Korea and two have been successful. The first part was signaling very clearly to foreign countries the strong ability of the United States to attribute attacks. Regarding the fact that numbskulls here are not persuaded—who cares? What matters is that Pyongyang, Beijing, and Moscow got the message. And they got this message from the United States: you are no longer invisible and you thought you could hide, but you cannot. And the second part of the response was, of course, putting in place punitive measures. The sanctions are part of that and I think they will have a good effect. Whether it will be enough of an effect...
remains to be seen. That speaks to the third issue, deterrence, which is the unsuccessful aspect of our response. We have had Admiral Michael Rogers, the Commander of U.S. Cyber Command, calling for stronger deterrence in cyberspace. I have started calling it “deterrence ancestor worship” because it is an idea from the distant past that was created for the Cold War. The Cold War ended twenty-five years ago, yet we are still trying to resurrect these aged concepts. The idea that somehow having a powerful cyber offensive will deter our opponents does not make sense. We have not figured out how to make deterrence work. We have been trying to energize cyber deterrence for almost a decade without success. Cyber deterrence has major limitations. A better approach—and this is where the rest of the U.S. effort comes in—lies in getting a multilateral agreement to build norms on responsible state behavior, identify penalties, and create a community of like-minded nations. That might be a more useful way to deter future attacks.

But again, other countries make a political calculation when they think about cyber attacks. Had the talks with Iran failed, I think the Iranians would have been emboldened to do more against the United States. The Chinese have difficulty calculating the risks of their actions. The Russians are in a much more aggressive mood. It is just not a happy picture. The North Koreans hopefully got the message, but you never know with them.

Journal: The executive order signed by President Obama on April 1 called on the Department of the Treasury to impose sanctions on actors that “engage in malicious cyber-enabled activities that create a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.” What do you think of the executive order?

Lewis: I think it is essential. You have to have penalties. Until the PLA indictments, you could count on one hand the number of people who have been punished for cyber crime. If you live in a Western country that enforces the law and you engage in cybercrime, you will go to jail within three years. In countries that do not enforce the law (like China and Russia), you run no risk. And the only time we have ever been able to arrest a cyber criminal is when that person was stupid enough to leave their home country of Russia and go on vacation in Thailand. If a known hacker decides to leave home, he or she will be caught. So, it is sort of a Darwinian thing for hackers. On cyber espionage, there was no penalty. I think the idea of creating penalties and linking that to attribution is key. Essentially, it is important to say, “We know who you are and we have the tools to punish you.” The indictments had a powerful effect in China. The Chinese were deeply upset by them, and I think that is okay if it is part of a larger engagement strategy and not a one-off. We need to recognize that it is not the 1990s, so the power relationship between the United States and China is different than it was in

---

the nonproliferation dispute. China is more powerful and more confident, and this will be a harder argument to win. Hard does not mean that the United States should give up, though, and so the executive order is a good step.

**Journal:** From your perspective, are there cybersecurity threats or issues that are under-reported or do not receive adequate attention?

**Lewis:** Sovereignty. There are two forces at play. One is that countries have realized that you can embed cyber issues in the existing framework of interstate relations, and that framework is based on national sovereignty. That is a powerful trend. The other trend is that the nature of interstate relations is changing because of the Internet. And the discussion has been a little dishonest because people have a goal. Someone says, for example, “I want the Internet to be open and free.” What does open and free actually mean? Well, it means the status quo, and that people should buy American products where the business model really limits consumer control. That is not a persuasive argument in other countries. We have political forces changing interstate relations that we do not fully understand and we have states realizing that they can put cyber issues in the context of interstate relations, even as they are changing. So that is a hard dynamic to figure out because you have these orthogonal forces. The near-term effect is that sovereignty will reshape Internet politics, and the long-term effect is that the Internet will reshape global politics. It is complex, it is dynamic, and it does not receive adequate attention.

---

**James Andrew Lewis** is a Program Director at the Center for Strategic and International Studies (CSIS). Before joining CSIS, he worked at the Departments of State and Commerce. He was the Rapporteur for the 2010 and the 2013 United Nations Group of Governmental Experts on Information Security. Lewis is an internationally recognized expert on cybersecurity and has authored numerous publications.

---

James Lewis was interviewed by Lara Crouch and Anastasia Mark on April 3, 2015.