property. And if cyber infrastructure is found on sovereign territory. A straightforward baseline conclusion might be that as a general matter territorial cyberinfrastructure is inviolable by other states. If operational realities or state preference requires otherwise, states staking out that departure bear a burden of persuasion and development of a new norm. Through decades and even centuries of practice and codification, such departures have been recognized in other domains such as the law of the sea transit and innocent passage regimes. The near future may see such efforts by states to identify exceptions to sovereign exclusivity with respect to the cyber domain.

A competing baseline, of course, is that there is no law. In the absence of significant state practice and especially lacking clear expressions of *opinio juris*, one might conclude either that a *Lotus*-inspired[14] rule of permissiveness operates or that there is simply no rule of conduct with respect to sovereignty in cyberspace at all. These are difficult propositions to reconcile with the now nearly unanimous starting point that international law applies to cyberspace. That conclusion, or concession if one prefers, becomes quite hollow if the answers to mixed questions of fact and law reflect a blank slate.

The *Tallinn 2.0* description of the current relationship between cyberspace and international law surely declines to express the adaptations and concessions to novelty that some would have liked to see. An important substantive and methodological question then is whether and how states will develop these adaptations and evolutions. If *Tallinn 2.0* manages to prompt or even goad movement from states in this regard, efforts to more clearly define and describe the relationship between cyberspace and international law, it will have been in some respects successful.

Remarks by Jeannie Rhee*

doi:10.1017/amp.2017.157

I come to this subject to talk about the unique intersection of state-sponsored cyber-activity with the private sector. Many of the costs of that activity are borne by the private sector that is domestically located in the United States, and there is often a disconnect between what is framed and developed in conversations and discussions by the United States and the reality on the ground within the private bar representing individual U.S.-based companies.

I should note that I speak just for myself, but I am informed by the experience that I and my partners have had in working in this space. Wilmer Hale has a robust national security cyber defense practice, and many of us have come to this practice with a background in government service.

In the private sector, within the private bar, all of us have collectively experienced the palpable disconnect between the discussions of this issue among states and the very different view of companies who are more often than not the subject of these kinds of cyberattacks. Just to tick off some notable examples, we might point to the Sony attack, which, notwithstanding the very close-in-time attribution by the United States that the hack came from North Korea, resulted in private domestic litigation and ultimately settlement on the civil side. We could also point to the public reporting regarding the financial consequences of distributed denial of service (DDoS) attacks, hack jobs, and possible exfiltration of information from any number of financial institutions we've represented, among them including JPMorgan Chase, in which 76 million records of

[14] The Case of the S.S. 'Lotus' (Fr. v. Turk.), 1927 PCIJ (ser. A) No. 10 (7 September) at 18 ("International law governs relations between independent States. The rules of law binding on States therefore emanate from their own free will … . Restrictions upon the independence of States cannot therefore be presumed.").

* Partner, Wilmer Hale.

personally identifiable information from its repositories were compromised, resulting in personalized notification and regulatory and law enforcement inquiries after the fact. Similarly, you see it on the health care side, or affecting platform providers or other data repositories and processors. And you see reports that even though there may be either light or hard state actor attribution, nevertheless, the immediate consequences are borne by U.S. companies. If there are any kind of state or federal obligations, or follow-on inquiries at the state or federal level, that is all borne by the private sector entities.

As a result, there is tension in the private sector–public sector partnership. The U.S. government obviously needs the information sharing, the participation, and cooperation of the obvious targets that are on the private sector side. Yet that relationship necessarily is fraught because it is the same monolithic U.S. government that will then conduct regulatory and other inquiries, notwithstanding state attribution, into the operation of private sector entities. The government will investigate the rigorousness of the private sector systems, the extent to which those entities are applying the duty of care with respect to its maintenance of sensitive information, and so on.

This is one of those challenges that is often lost in the discussion at the one-hundred-thousand-foot level about how to deal with cyber-activity as a matter of statecraft and state-to-state relations under international law. But when you focus on the immediate consequences of this cyber-activity, when you see its immediate consequences trickle down to those entities here in the United States, it becomes a more complicated relationship. It is certainly a difficult one for the United States government to navigate in balancing its broader objectives and interests.

Laura Dickinson

Let me now pose a series of questions on a few different topics. The first one addresses the status of the *Tallinn Manual*. It seems as if we have a manual for every area of law we can imagine. For example, there is a forthcoming space law manual, and many other manuals. Is this really a productive way to identify the law in this area? And, specifically for Jeannie Rhee, is *Tallinn* relevant to your practice?

Jeannie Rhee

The short answer is no, not really. The two parts of this panel (the public sector portion and the private sector portion) do not intersect with each other as much as they should. It is imperative that we open up that conversation a bit more because obviously *Tallinn* should matter to those companies that we represent in the private sector, but it is not clear that it does at this moment in time. At the end of the day, we have a robust domestic legal regime that all of these companies are subject to. So first and foremost, given the mountain of domestic legal responsibilities and potential vulnerabilities, and legal exposure, that these companies face, necessarily, in the private sector, we start there.

Gary Corn

Consistent with a post I put up after the launch of *Tallinn 2.0*, I would say that it is an excellent piece of work. I believe it is helpful to advancing the thinking in the field, especially in a new area like this, where people who are well versed in international law on various subject matters can put some good thought on how those regimes will apply. Pulling all that together in a single source is very helpful. That doesn't mean that, from each state's perspective—from the perspective of attorneys advising policymakers in the government—we necessarily think *Tallinn* got everything right. It is certainly helpful for understanding the views out there and understanding the issues. It

https://doi.org/10.1017/amp.2017.157 Published online by Cambridge University Press

provides a healthy starting point and is a valuable source. I should also confess that I was one of the numerous peer reviewers in that process.

Far be it from me to speak for the private sector, and Jeannie has a much better perspective on it than I do. But I do think *Tallinn* should be of interest to the private sector for a variety of reasons. First, there are implications to the particular courses of action the private sector might seek to take in this area. There are a variety of views out there. I have heard from different ends of the spectrum in the private sector. In some quarters, there is growing frustration, understandably, that they are not being protected and therefore desire active defense measures. In other words, there is a desire to be able to take actions outside, to "hack back," so to speak. That certainly has domestic law implications, but it also has international law implications, for example for questions of state responsibility. If it happens in the course of, or at a level that might be construed as initiating, armed conflict, it implicates questions of direct participation and could put companies and employees at a degree of risk they may not be thinking about. It is important for companies to consider, in their engagements with the government, what the right protective regime should be overall and what views the government ought to express about *opinio juris* on these matters. The impacts on the private sector, the need for protection, and these kind of questions would factor in.

Sean Watts

There is certainly a proliferation of these manuals. It starts all the way back with San Remo manual on the law of the sea. There is also a manual on noninternational armed conflict, an air and missile manual, and a forthcoming space manual. I am still in the army reserves, and it was encouraging to go the place I am assigned in the reserves and to see dog-eared copies of the *Tallinn Manual* in every cubicle. Yet such use of *Tallinn* presents a level concern as well. One wonders, why do these lawyers need this source? Probably it is because they do not have all the sources they need from their own government. One of my ulterior motives in participating in both *Tallinn* manuals was the hope that it would prompt feedback from governments, that governments would either react to the manuals, or, even better, replace them. If governments were willing to write something of comparable scale and depth, I think government lawyers practicing in this area would be well served by that.

I do concur with Gary on the point about the relevance of *Tallinn 2.0* to the private sector. They were not a strong voice, and it is probably our fault and theirs. I do not think we made an aggressive effort to reach out to them. For precisely the reasons Jeannie mentioned, because they are the victims and the cost-bearers of some of the statecraft in the area, they do have a stake in the game. If they thought about it carefully, they might realize that they have some power to influence state views, either to pressure states to make their views known or even to subtly shift the law. If they feel an inadequacy in international law is at all responsible for those enormous costs, why wouldn't they lobby government? Why wouldn't they pay attention to products like this, and make their views known?

Laura Dickinson

Now let's turn to some questions about state responsibility and the role of nonstate actors. Does the existing regime of state responsibility, on the one hand, and domestic criminal accountability, on the other, adequately protect against and deter actions by nonstate actors? In particular, for Jeannie, are the current restrictions on hacking back sufficient to protect corporate interests, and what is your view of the potential implications of self-help for potentially triggering some of the international legal rules?

https://doi.org/10.1017/amp.2017.157 Published online by Cambridge University Press

Jeannie Rhee

I would note that, based on reports of a sophisticated client that is subject to an onslaught of daily activity in the form of a multitude of attacks and who tracks all of it, year in and year out you see the massive dip in activity around the Chinese calendar and Chinese New Year. That is just the reality. There is a disconnect between what certain states are doing and the U.S. government perspective as is reflected in the previous comments about what is and is not permissible both under domestic law and certainly under international law as it has developed regarding cyberspace. Where does that leave us here in the states when you are a private company? The government has been good in many respects. It is reflected in the public indictments of the state attribution, and in efforts to apprehend some of the bad actors, and to identify them, and take recourse. But it does not even come close to capturing the day in and day out onslaught of state and quasi-state activities that U.S. companies are subject to. The frustration is only going to continue to grow. This kind of activity is not going to dissipate. It is only going to increase. There are only a few companies, notwithstanding the talk, that are able to begin to think about engaging in self-help. Certainly it is incredibly fraught. If there are lawyers in the room, any one of them can rattle off all of the ways self-help is an incredibly fraught exercise even as hypothetical-scenario tabletop planning. The reality is that the private sector needs to participate with the U.S. government to develop a more robust defensive regime rather than sit back and hope for the best when the onslaught comes.

Gary Corn

From a deterrence perspective, I have two points. First, I think we see more broadly outside of cyber that deterrence is not particularly effective for dealing with nonstate actors. The motives of nonstate actors are fundamentally different from those of states. To be sure, there are different types of organized nonstate groups. In general, deterrence doesn't seem to be effective, and so the real question is whether the legal framework is adequate to enable states to counter the threats. Even with respect to states, the evidence to date shows that they are not being deterred. We are seeing increasing levels of activity that shows states are seeking to exploit this domain with varying degrees of aggressive behavior, from DDoS's in the financial sector to the Sony incident, to achieve strategic objectives. These incidents point to the need to be able to counter this activity at some level. Deterrence theorists may be better positioned to speak to this question. But in general, countering cyber through cyber alone is not necessarily effective. You need to look at a broader deterrence strategy for states. There is a counter activity imperative there, as well. In this grey zone, actors are exploiting ambiguities. And, particularly relevant for us here, there are ambiguities in the law. As much as I do credit *Tallinn 2.0*, it is not a definitive statement, nor can it be because it is not a statement by states. We need greater clarification from states. Such clarification is always a challenge because states approach that glacially. They must balance whether clarification inures to their benefit or not. Furthermore, the legal framework is rooted in the nineteenth and twentieth centuries. It is solid, but it needs to go through an adaptation process to deal with this new technology and this new environment.

Sean Watts

I agree our legal framework is chiefly a nineteenth- and twentieth-century framework. This fact points us back to the question: How adequately or inadequately does this area of law address nonstate actors? In my view, it really doesn't address them very adequately at all. The *Tallinn* Manual concludes that the vast majority of international law rules are rules for states. There are maturing views among international lawyers that envision more robust roles for nonstate actors in the

https://doi.org/10.1017/amp.2017.157 Published online by Cambridge University Press

formation and operation of law. But it was the majority view at *Tallinn* that we are not there yet. If states were to choose to grow the law in this area, it would be a worthwhile investment, whichever direction they took it. To step back to another methodological point, I agree with Gary that, before a state decides whether it wants to weigh in on law or clarify law, there's a threshold question: Does clarification stand to advantage us, and will we be better off if we clarify the law, or do we like the operational flexibility we enjoy through this silence? Whether one wants flexibility, or whether one seeks more active regulation, in my view, silence from government is the incorrect answer on both counts. That is, even if ambiguity serves the interest of a state, that ambiguity needs to be actively preserved, especially in the face of projects like the *Tallinn Manual*, doctoral dissertations, academia, or courts and tribunals, all of which are seeking to bring more clarity to this area. States do not achieve or maintain that ambiguity, or preserve those voids, by remaining silent. They preserve the void by also actively defending the void. They must assert that the void is here, that it is a void. It is a void for a reason, and we continue to support that void.

Gary Corn

Let me give an example in the nonstate actor realm that highlights some of the gaps in the current framework. If you had polled a body of national security law experts prior to September 11, 2001, you would have found some, perhaps, that would have identified the unwilling-unable test and analysis as a justification for taking actions against nonstate actors in third-party states as a matter of self-defense. But they would have been a relatively small minority. The law just had not seen an event or circumstances that pushed that question prior to that date. But certainly after September 11, 2001, while not all would agree, you would get a different view. So here is an area in which the law has had to adapt to a very new circumstance. Now, that was adapting notions of what had previously been historically part of the law of forceful reprisals into the self-defense framework and justification as an exception to the prohibitions in the UN Charter on use of force in armed attack. That does not in present form exist, for example, for the law of countermeasures. And so you have a very odd dynamic. Nonstate actors use infrastructure on the Internet that is distributed across multiple countries. What does the law say about a victim state's right and ability to take action? Even if you are arguably in the course of armed conflict with a nonstate organization, but in that third-party state—to deny and deprive that nonstate group from using that co-opted infrastructure could be unlawful. Sometimes it is purchased infrastructure. Countermeasures are otherwise unlawful acts below the threshold of the use of force. They are limited to taking an action that is unlawful only in the face of a violation of international law itself against you as a victim state. And they are only available against a state. So unless you can find a third-party state to be in breach of an international obligation to you, you would seem to be left remedy-less, without options in that circumstance. Somewhere, the law has got to give in order to address that kind of situation.

Laura Dickinson

I'd now like to turn to the thorny question of sovereignty, and how robust a principle it is in prohibiting or permitting cyber-actions. Sean has articulated another view. For Gary, I wanted to ask whether you'd like to respond to that. For Sean, how does your view square with state practice? For Jeannie, the question is, what view of sovereignty is best for the private sector?

Gary Corn

Sovereignty is no doubt both a foundationally and extremely important principle in international law but a complex one subject to different interpretations both as to its qualitative nature as a

https://doi.org/10.1017/amp.2017.157 Published online by Cambridge University Press

binding norm or not, as well as its parameters. And there are different aspects to sovereignty as well that add to the complexity of the discussion. But at its heart, there is a question as to whether sovereignty is itself is a primary rule or norm of international law that itself can be breached, or whether it is a general principle that speaks more to the legal personality of states upon which primary norms are developed through the international law-making process among and between states. I don't think it is a secret that my personal view is that it is the latter, that it is a general principle. States have exercised their right of sovereign equality as a foundational principle of international law to agree to certain rules that prescribe actions vis-à-vis one another, such as the *ad bellum* regime reflected in Article 2(4) of the UN Charter, as well as the customary international law norm of nonintervention, which has constitutive elements and thresholds that states have agreed to with respect to their behavior. Below that, it is a much knottier question, and I believe there is not sufficient evidence to say that there is a rule that can be breached there.

Sean Watts

The view of sovereignty in *Tallinn*, that sovereignty is not only a principle but also a rule that prohibits interference with the independence and exclusivity of states, came to us late in the publication process, and was something of a surprise. I have to admit, it is sometimes difficult to square with state practice. If it is a rule, it is sometimes breached. These are murky areas. States are usually trying to hide it when they do this, and I am not sure we have a complete picture of state practice in an unclassified realm. Similarly, asking *Tallinn* to square up with state practice in terms of sovereignty asks *Tallinn* to prove a negative in some respects. Where are all the opportunities states have had to violate sovereignty but do not in fact violate sovereignty? If we were to do a quantitative analysis, I suspect the number of occasions in which states have declined to violate sovereignty, perhaps out of *opinio juris*, would outnumber the situations in which they have violated sovereignty. There was no significant feedback on this issue in the Hague process. The sovereignty chapter was circulated to states, yet no state took issue seriously with the position the Manual asserts on sovereignty.

There is a serious view out there now, a January 19 memo issued by the Department of Defense general counsel, which lays out a very clear position on sovereignty. It concludes that the threshold of wrongfulness (recall Gary's discussion earlier about countermeasures) stops at the prohibition of intervention. It notes further that of course uses of force are internationally wrongful, and that even violations of the prohibition of nonintervention, the coercive interference with the external affairs of a state, are internationally wrongful acts. But the memo, somewhat surprisingly, if understandably given the operational realities, concludes that activities below that threshold are not regulated. There is a challenge and a reconciliation that has to happen there. If that is a newish view—not as a question of law but rather as a mixed question of law and fact, what is the incubation period? Can a state immediately draw such a conclusion? At what point are we dealing with a rationalization? And at what point are we dealing with legislation? That is a thornier methodological question.

Jeannie Rhee

Again, I should note that I am just speaking for myself. On the question of sovereignty, from the perspective of one of the U.S.-based victims, sometimes it feels as if it is a one-way ratchet—given the basic infrastructure of the Internet and the operational reality that you immediately run into someone else's border, and that there is an almost impossibility of getting to any defensive measure. Given the operational realities, this is a very interesting debate and an important one in international law. But here on the ground, there is nothing that can be done by U.S. companies without the U.S. government figuring out a way to be proactive in this space.

https://doi.org/10.1017/amp.2017.157 Published online by Cambridge University Press