2020

The Promise and Limits of Cyber Power in International Law: Remarks

Monica Hakimi
Columbia Law School, mhakimi@law.columbia.edu

Ann Väljataga
NATO Cooperative Cyber Defence Centre of Excellence

Zhixiong Huang
Wuhan University School of Law

Charles Allen
U.S. Department of Defense

Sue Robertson
Attorney-General's Department Australia

See next page for additional authors

doi:10.1017/amp.2021.79

THE PROMISE AND LIMITS OF CYBER POWER IN INTERNATIONAL LAW

This panel was convened at 2:15 p.m., Thursday, June 25, 2020, by its moderator Monica Hakimi of the University of Michigan Law School, who introduced the panelists: Sue Robertson of the Office of International Law, Attorney-General's Department Australia; Charles Allen of the Office of General Counsel, U.S. Department of Defense; Zhixiong Huang of Wuhan University School of Law; Ann Väljataga of the NATO Cooperative Cyber Defence Centre of Excellence; and Doug Wilson of the UK Government Communications Headquarters.

Introductory Remarks by Monica Hakimi*

Hi, everyone. I am Monica Hakimi from the University of Michigan Law School, and I would like to welcome you to our panel on cyber power and its limits. The topic almost does not need an introduction. We all know just from reading the news that our collective dependence on cyberspace is also a huge vulnerability, and state and non-state actors exploit this vulnerability to do one another harm. They use cyber technologies not just to spy on one another, but also, for example, to interfere in national elections, to steal trade secrets or other valuable information, to disrupt the activities of political, military, or economic institutions, and at times to cause physical destruction or death.

Moreover, because these technologies allow the perpetrators to obscure their identities or the full effects of their operations, the people and institutions that are affected do not always have the relevant information to protect themselves from future attacks or to respond.

In 2013, a group of governmental experts stated that "[i]nternational law, in particular, the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible information communication technologies (ICT)."[1]

Later instruments have confirmed and elaborated slightly on the premise that the general principles of international law apply in the cyber domain, but there continue to be questions about how it applies and how it might be supplemented by other non-binding norms to regulate cyber conduct. These are the questions that we want to explore today.

I am delighted to introduce our panelists, which I will do relatively briefly in order to save time for discussion, and I will ask, given our format, that you raise your hand as I introduce you so our viewers can identify you. First, we have Charles Allen, who has served as deputy general counsel for international affairs at the U.S. Department of Defense since 2000; second, Zhixiong Huang, who is a professor at Wuhan University School of Law and has served as one of the experts who worked on the *Tallinn Manual 2.0* Cyberspace Law Project; third, Sue Robertson, who serves as first assistant secretary of the international division in the Office of the Attorney General of

* University of Michigan Law School. What follows is a slightly modified transcription of the panel presentation.

[1] UN Doc. A/68/98, para. 19.

Australia and has previously served in the Australian Department of Foreign Affairs and Trade; next, Ann Väljataga, who has served as an international law researcher at the NATO Cooperative Cyber Defence Centre of Excellence since 2016; and last but certainly not least, Doug Wilson, who was formerly the legal director at the Foreign Commonwealth Office and is now at the UK Government Communications Headquarters.

We have decided to organize this panel more as a conversation than as a series of presentations. I will pose some questions to the panelists to facilitate the conversation among them, and will incorporate as much as possible some of the questions that ASIL received through the online format in anticipation of this panel.

To start, I want to focus on the question of what activities when conducted by states in the cyber domain are internationally wrongful. Ann, perhaps I could start with you and ask this question: when one state uses another state's territory to engage in some kind of cyber conduct—for example, to use its servers—without that territorial state's consent, does that, per se, violate some principle of international law, such as the principle of state sovereignty or territorial integrity?

Remarks by Ann Väljataga*

According to my reading of the *Tallinn Manual*, it still seems that there are many determinant factors regarding manifestation of the use of cyber infrastructure, and if the manifestation itself brings about something that could be described as violation of sovereignty, then yes. But at the same time, this is not a crystallized principal rule, and when you compare this kind of position to what the law says or what practice even says in other domains, then we see that it is a bit in conflict because, for instance, the mayor trespassing into the area of territory of another state is breach of sovereignty. Therefore, it is still up there, but most likely it will depend on the manifestation. If the uses are peaceful, as such, then probably it would not be described as a breach of sovereignty.

But then again, we come to maybe the major apple of discord of cyber law in these states. It is whether sovereignty as such can be breached, or is it merely a guiding principle and not a rule that you have to obey or you are violating it?

Monica Hakimi

If I am understanding correctly, you are saying that there is a question about whether the mere use of another state's territory without its consent violates state sovereignty and is unlawful for that reason or needs to violate some other principle of international law to be unlawful. Is that correct?

Ann Väljataga

The thing is what does consent mean. If, for example, one state is using the servers that are located on the territory of another state, yet still operated by a private actor, and they are using them for peaceful purposes or even, as some experts have claimed, for perhaps purposes of interception of espionage, then whether or not it is a breach of sovereignty is still disputable.

Monica Hakimi

Zhixiong Huang, I saw you gesture. Did you want to jump in?

* NATO Cooperative Cyber Defence Centre of Excellence.

https://doi.org/10.1017/amp.2021.79 Published online by Cambridge University Press

Remarks by Zhixiong Huang*

I think this question very much depends on how sovereignty and territorial integrity is to be defined and interpreted in the cyber context, and we can see states and scholars do have quite different views. For example, if we look at the position paper released by France last September, it states "any cyberattack against a French digital system or any effect produced on French territory by digital means" attributable to another state would constitute a breach of French sovereignty. Then very likely for France the answer would be yes. But as was mentioned just now, there are also states holding that sovereignty is not a rule of international law containing concrete obligations. So for them, the answer, I think, would clearly be no.

China, as far as I know, has not yet made its position very clear, but my understanding is it is likely China will be, more or less, in agreement with the French position.

Monica Hakimi

Chuck, please go ahead.

Remarks by Charles Allen**

Yes. Thank you very much. I noted that Ann mentioned the dichotomy between sovereignty as a rule and as, on the other hand, a principle, and that was also discussed by our Chinese colleague. What I would like to say is that in the United States, we really try to grapple with these almost intractable issues, as Monica mentioned at the outset. In a series of speeches by U.S. officials going back to Legal Adviser Harold Koh in 2012, Legal Adviser Brian Egan in 2016, and then most recently in more of a shortened version by the general counsel of the Department of Defense, Paul Ney, we have addressed these issues. I also note that the UK attorney general in 2018, in a very persuasive speech, addressed these issues as well.

Our view, at least at this point—and we understand things are evolving—is that there is not a sufficiently widespread and consistent state practice, resulting from a sense of legal obligation, to conclude that customary international law generally prohibits such non-consensual operations in another state's territory. This conclusion is with the important caveat that the action, the "intrusion," if you will, does not constitute a prohibited intervention or use of force. That is, the action does not interfere in violation of Article 2(4) of the UN Charter in a country's right against incursions on its territorial integrity or political independence.

I think that the UK attorney general's speech is particularly persuasive on this point in saying that sovereignty is, of course, fundamental—and the United States agrees with that—to the international rules-based system. But we do not see that there is a rule as a matter of current international law that prohibits us from, as the United States has said recently, being able to "defend forward," perhaps including with incursions in other countries, to protect such vital elements as elections, election results, the integrity of the election process.

Monica Hakimi

Okay, wonderful. Thank you. Sue, let me turn to you. First, do you want to state Australia's position on this particular question? Then, let us move to a more specific question. If we accept, as some

* Wuhan University School of Law, China.

** Office of General Counsel, U.S. Department of Defense.

https://doi.org/10.1017/amp.2021.79 Published online by Cambridge University Press

argue, that cyber conduct does not necessarily violate a general sovereignty norm, can we get any traction out of the principle of non-interference? Let us focus on conduct that interferes in a national election. What kinds of election interference might actually violate the principle of non-interference? Must the interference involve an element of coercion to violate it? And if it so, what qualifies as coercion in this context?

Remarks by Sue Robertson*

Thanks, Monica. I think in relation to this issue of the rule or the principle of sovereignty, like the UK and the United States, Australia's position is we are not quite there yet, that this is a contested view. Some states—such as France and the Netherlands—have said they are in favor of it. We do not have a public position as of yet. We think the question is a challenging one, but that state practice is basically still evolving in this area.

I might also pick up on something our Chinese colleague, Professor Huang, just mentioned as well, that the issue of interpretation of the different principles is key here. For example, it may be that, depending on a state's interpretation of prohibited intervention, there may not be a lot of difference in practice between a violation of sovereignty and a violation of prohibited intervention, but it depends on where those lines are actually drawn.

But, of course, Australia does believe in the principle of state sovereignty in cyberspace, and obviously, a state has sovereignty over its cyber infrastructure, for example, located on its territory and the cyber activities that it does on its own territory.

You raised the question more specifically of electoral intervention, which is a classic gray zone area where there may be a whole lot of activity that goes on that is not internationally wrongful and falls short of a prohibited intervention. I should say that for states, cyber interconnectedness has raised the stakes on a whole lot of critical infrastructure and governance processes, not just elections, and a huge focus of legal advising is on how to protect that critical infrastructure that can obviously affect millions of people and their well-being, in terms of hospitals, electricity, finance, and those sort of realms.

I think it is important to say that states do have a variety of tools, and international law is one of them. But turning to this issue of prohibited intervention, as we know, it has two components, two constituent parts. First, a state must interfere by coercive means, and they must intervene in the *domaine réservé*, something that is essentially within the right of that state to control and choose. We have talked about this in various ways, and I would say that out of *domaine réservé* and coercion, coercion is generally the more difficult to advise on. I think that is because it is still an indeterminate concept in some ways. It cannot be merely persuasion or pressure. That is just a matter of statecraft. We know from *Nicaragua* that it goes to this issue of states' choices, which must remain free ones.

Just quickly, on the example of elections, I think Australia would agree with the UK Attorney General and others who have said this, and our Attorney-General has also made some statements on it, that cyber operations that manipulate an electoral system would satisfy that test. And I think others, including the Netherlands and the UK, have agreed on that. But I think it is an open question, the extent to which other types of interference in elections actually reach this threshold or not, and perhaps we could talk about interference in the U.S. democratic elections, for example, in 2016 in which the U.S. government did not respond by characterizing those necessarily as an international

* Office of International Law, Attorney-General's Department Australia.

https://doi.org/10.1017/amp.2021.79 Published online by Cambridge University Press

wrong. They took a lot of other steps, using tools such as sanctions and criminal prosecutions and so on. So I think that does raise the issue. That does show how difficult this issue can be.

Monica Hakimi

Doug, please go ahead.

Remarks by Doug Wilson*

Thank you, Monica, and thanks to you and ASIL for having me. It is a real pleasure to be alongside such distinguished fellow panelists, many of whom it is a pleasure to see again.

I just wanted to take us back, if I may, to the conceptual elements of what we are discussing. We are discussing the promise and limits of cyber power under international law, and I think it is important, just briefly, to dwell on what cyber power means. For the UK, we have been positing a public vision of what that concept entails, and there are three parts to it. There is the ability or the capability to protect the digital homeland, the cybersecurity element. There is the capability to project power and influence through cyber means to disrupt what adversaries are doing, for example, when the nation is threatened. Underpinning that, there is the legitimacy of strong legal regimes at the domestic and international level. I think when we are discussing this, we ought to just bear in mind those component parts because what you do in one area and how you describe what has been done to you can affect your own ability to act. As international lawyers, we need to keep that balance in mind.

For me, the way you introduced the first question, I thought was absolutely spot on. The real question we ought to be asking ourselves is a particular act or series of acts or line of activity internationally wrongful. As international lawyers in this space, we are often quite concerned with the means of transportation rather than the destination. So we can have arguments about sovereignty and how it materializes in terms of specific rules according to some or into what everyone agrees is the rule around the prohibition on interference in internal affairs.

For the UK, the question really is whether the threshold of the prohibition or non-intervention has been met in a particular case, and what we tried to do alongside other countries—the United States, Australia, France, Netherlands, Estonia, and probably others in the mix too—is populate the space with specific examples of what activity we think is internationally unlawful. We recognize states can arrive at that destination, as I say, by different means.

The election example, as Sue has already said, is a really hard one. In the speech by our Attorney General that Chuck was kind enough to mention—thank you, Chuck, flattery will get you everywhere—we deliberately couched that as manipulation of an electoral system with the aim of altering the result. So what that does capture obviously is with voting registers, electronic voting, postal voting, all of those kind of things, but where there is more scope for progressive development or further discussion is around really tricky issues like disinformation and the whole host of issues that Sue touched on in her intervention.

So for the UK, what we are really keen to do is see that space, the space of what is internationally wrongful, populated by real discussion of both types of examples. I know we are going to come on to some others, but what is unlawful in this space? What are the rules of activity in this area of statecraft that we are all seeing develop and be used for, as you said in your introduction, rather subversive means where countries are trying to disrupt and mislead states or their populations in a

* UK Government Communications Headquarters.

https://doi.org/10.1017/amp.2021.79 Published online by Cambridge University Press

really unhelpful way? How can we bring some order to that, and how can we set up the rules of deterrence and proper conduct?

Monica Hakimi

That is great. I would like to take you up on that suggestion and home in on a specific example. Let us say there is a massive disinformation campaign that causes a population to call into question the election results, but there is not significant evidence of tampering with the machinery of the election or the counting of votes. Would that, in your view, violate some principle of international law? That is my first question.

My second question, just to have two on the table, so I do as little talking as possible and you all do as much as possible, is to what extent must states affirmatively prevent wrongful conduct, however it is defined, when conducted not by their own state agents but by some non-state actors either in their territory or outside their territories? This is what is sometimes called a "due diligence obligation." To what extent do states have a due diligence obligation, an obligation to exercise due diligence to prevent non-state actors from engaging in harmful cyber conduct? And then, how do we define the specifics of any due diligence obligation, to the extent that one exists?

So, Doug, since you raised the question, maybe I will come back to you and then do a round robin with the other participants.

Doug Wilson

To answer your extremely hard question, it is possible that it could definitely reach that level of a prohibited intervention, and a lot would depend on the facts.

But I would come back to what Sue said earlier. International law is one of an array of relevant frameworks here and tools that can be used to combat that kind of thing. A lot depends on the persuasive effect you can have on social media companies or big tech. The active targeting of misinformation is not currently within the domestic regulatory framework, although around the world you can see more interest in firming up the rules of the game and who is responsible for what.

You know what we are seeing right now in a number of places across the world? Big tech and social media companies taking a much more proactive approach to this, which in itself carries a whole host of tricky issues to answer.

When it comes to responsibilities around what is termed "due diligence," of the UK, there is no doubting that states have an obligation not to allow in a knowing way the territory to be used for acts contrary to the rights of other states. We can go back to *Corfu Channel* for that proposition, Whereas, there is a lot more caution for us around due diligence as the content of any such rule as a good international lawyer working for a government. You want to be sure when you are accepting the emergence of a new rule or adaptation of rules from one area of international law to another. What does it really mean, and what does the content of that rule say? Because what we would not want to do is oblige states to apply such levels of due diligence so that only a few states with a really cutting-edge system of cybersecurity would be able to meet them. I do not think there is any value in that, so, again, I am interested in what the content of any rule that is termed due diligence might actually be. But there is no doubting underlying general international law obligation by use of territory, and it is just how it applies and what the standards are in that space.

Monica Hakimi

Sue, do you want to follow up?

https://doi.org/10.1017/amp.2021.79 Published online by Cambridge University Press

Sue Robertson

Thanks, Monica. I think Mike Schmitt looked at these issues really well and talked about both views. In one example, if an election result is not manipulated, is that sufficient to reach the level of a prohibited intervention? But he then put forward the other view, that misinformation can actually cause events to unfold in democratic processes that would otherwise not have occurred, and I think there is definitely some merit in that. But it also highlights the real sticky problem we face that the effects of various forms of indirect and direct misinformation and malicious cyber activity may not be known until a particular time, and so as time unfolds, things may actually get worse. I know there has been some interesting commentary on that recently about interference in elections where the effects can actually become worse over time. So we are left judging at a particular point in time.

I think that the fact that a state does not characterize an activity as meeting a threshold does not necessarily mean that they do not share that view that it does. It is a bit of that "secret life of international law" that Daniel Bethlehem talks about so well. For a whole variety of reasons, they may not have decided to characterize an activity in a legal way, whether it is to protect a source or because they can achieve their political shaming through another mechanism.

Due diligence is a really good example. It is one we are still thinking about and it will become increasingly important as attribution just remains so difficult. Our view is that it is unclear the extent to which states are obliged to exercise due diligence, and that is because of that lack of crystallization. That is why we have been really supportive of the development of norms and more soft principles through the UN Group of Governmental Experts and other processes because we believe it is definitely worth exploring and taking a realistic approach, as Doug has already mentioned. I think that it is important to actually say what would be expected for due diligence and what level of knowledge is required. There are interesting questions about constructive knowledge as well. There are a lot more questions than answers for us at this stage, but I think that even putting to one side legal characterizations, politically, it is going to become harder and harder for states to ignore the harmful activities that come from their jurisdictions.

Monica Hakimi

Chuck, did you want to weigh in on that question?

Charles Allen

Yes, just briefly, because I think that Douglas and Sue really handled it about as well as one can. It is an intractable problem to know whether a disinformation campaign amounts to the kind of coercion that would be actionable. I appreciate Sue's very clear statement of the International Court of Justice *Nicaragua* case principles, which would apply.

Some of the U.S. Department of Defense's thinking has been made clear particularly in General Counsel Ney's speech in March 2020, not necessarily in the international law part of the speech, but in talking about the U.S. approach in attempting to deal with the interference that has occurred. Once again, we describe it as "defend forward." We believe that it is appropriate to be able to defend forward, including, consistent with the principle of sovereignty, but nevertheless to be able to defend forward to counter foreign cyber activity that targets the United States—the case in point being the integrity of the election process. We believe that this indeed comports with our obligations and our commitment to a rules-based international order. But, again, I am not sure I can add very much substantively to what Sue and Doug said.

https://doi.org/10.1017/amp.2021.79 Published online by Cambridge University Press

On the due diligence question, the U.S. statement as part of the UN Group of Governmental Experts (GGE) work in 2016–2017 indicated that we did not see that there was an obligation of due diligence. I think it is generally true that states are not exercising due diligence. So from a perspective of custom and practice, it is hard to say that there is that obligation.

On the other hand, it is just as true that, as has been said, states do not have a right to conduct or harbor in their territory cyber activities that are used to harm other states. Again, we would say that U.S. efforts, including defending forward, to counter such activities would not be a violation of the principle of non-intervention.

Having said that, and suggesting there is not an obligation of due diligence, I do think that the sovereignty principle reflects that there are both responsibilities and authorities. If an activity is conducted within a state's jurisdiction, the state has certain accompanying duties to ensure the activities are not used to harm other states, for example, in violation of Article 2(4) of the Charter.

Monica Hakimi

Okay, great. Let s shift from the question of what conduct is prohibited or required of states and turn instead to the question of how states may lawfully respond in the event that they are affected by some cyber conduct? Let us start with the difficult question of when cyber conduct qualifies as an armed attack, so as to trigger the right to use defensive force, whether collectively or individually.

To be as specific as possible, I will put this scenario on the table. Imagine a situation in which a cyberattack does not cause physical destruction or death but rather, for example, causes a military installation to stall out for an extended period of time, such that that installation is inoperable, not in the midst of an armed conflict but in ordinary times. Would that attack qualify as an armed attack so as to trigger the right to use defensive force, or must the cyberattack cause significant physical destruction or death in order to trigger that right? Zhixiong, maybe I could start with you and get your views on it.

Zhixiong Huang

I think the issue of what constitutes an armed attack in the cyber context has not yet been settled, and the law is still evolving. Overall, I think the determination will have to be made based on a case-by-case assessment, taking into consideration such factors as scale and effect and also other factors like the intention of the operation.

But I do not think we can conclude definitely that if a cyber operation caused damages or death, then it would constitute an armed attack. For example, if a police officer or a member of the army of State A intentionally kills a national of State B without further justification, in my view, this would be an internationally wrongful act of State A, and legal responsibility will incur. But for the purpose of our discussion, this may or may not be seen as an armed attack. This is what I understand the situation in the real world, but in cyberspace, how can we definitely conclude that as long as a cyberattack caused death or physical damage, then it is an armed attack? It is my view that a number of factors should be considered.

Monica Hakimi

There are two questions on the table. One is at what point a cyber act that actually causes physical destruction or death amounts to an armed attack, and a second question is whether it is ever possible for a cyber act that does not cause physical destruction or death but causes some other harm—and I am using a harm directed at the military because that seems like the most obvious kind of other harm—to amount to an armed attack. With those two questions on the table, what I will do is

https://doi.org/10.1017/amp.2021.79 Published online by Cambridge University Press

ask our governmental experts to weigh in, and then, Ann, I would like to come back to you when we talk about countermeasures. Chuck, please go ahead.

Charles Allen

I believe your question is pointing not necessarily to the worst types of cases such as, for example, causing a failure that triggers a nuclear plant meltdown, where there would not be doubt about whether it constituted a use of force. Also, a cyber act that opened a dam above a populated area and drowned people below would clearly be a use of force. As Professor Huang just indicated, we would have to look at the facts as they come, on a case-by-case basis. One can imagine a cyber action that might cause a physical effect but that would not necessarily amount to a use of force. On the other hand, to address your second scenario, I can see a case in which a cyber action may cause no physical effect—for example, does not harm people by shutting off oxygen to a hospital's patients who need it to survive, and people die—but rather, let us consider the situation you posit, talking about military systems. A country has a right to use its armed forces to defend itself, and it needs to be prepared to do so as situations and threats arise. If, as a result of a cyberattack, let us say even the logistics systems of the military are imperiled, are immobilized, so that the country's ability to conduct and sustain military operations in its own defense, in its own national interest—I think that could be considered a use of force under *jus ad bellum*, which may warrant a response that would be subject to the requirements, as always, of military necessary and proportionality.

Again, it would have to be looked at based on the facts presented. Let us say that the cyberattack slows down the logistics system by three days in its deliveries to the forces—then probably this would not warrant a response in self-defense. On the other hand, if the attack truly crippled the logistics systems so that your airplanes cannot fly, your ships cannot sail—then that might be a different story.

Monica Hakimi

Doug?

Doug Wilson

Thank you, Monica. If I may say so, I feel for your students because you are always asking these really hard questions. I agree with what Zhixiong and Chuck said.

I would add two extra points for my own perspective. One is underscoring the intent point. Did the attack aim to do something more, and did cybersecurity or luck or whatever actually prevent that harm? Because you ought not to be punished as a state or restricted in your response because you are able to defend against an attack that was going to do something much worse. That is part of the consideration that has been laid out already.

The second point I would make is, does it matter? Because what are you looking to do back, or how are you looking to respond? Are you looking to use diplomatic means? Are you looking to use other means of exerting pressure like sanctions? Are you looking to take cyber activity in response, in which case you would use the framework that applies here for the UK? That would be what is permissible around our domestic legal framework, which is very tightly constrained and has considerable independent scrutiny.

And then what does international law permit in these circumstances? If you are signed up to a rule of sovereignty that is very constraining, that will limit you, and you need to go through that gateway means in order to justify any response. Whereas if you are applying the approach that

https://doi.org/10.1017/amp.2021.79 Published online by Cambridge University Press

Chuck outlined earlier and that General Counsel Ney has talked about, that our Attorney General has talked about, you have got more freedom of maneuver in the cyber world to respond to these types of things without having to pin down exactly what has happened to you—in the way that would help me avoid answering your really difficult question.

Monica Hakimi

My students try to do the same thing. Sue, would you like to weigh in on this question, or would you like to move on to the question of countermeasures? I think Doug teed up the next question by saying that, in many circumstances, states will choose not to respond with force. They will choose to take other measures, and that brings us to countermeasures.

Sue Robertson

Yes. One point I just wanted to make is that, as fascinating as questions of international humanitarian law and the use of force are—and we all love writing and reading about them—the use of force and IHL are not the bread and butter of my advising day to day. I would say the gray area probably takes up 99 percent of my time. That does not mean that questions of IHL and the use of force are not important, but I think it does go to Doug's point. Of course, how you characterize things matters, but I do not think states are looking to characterize things as a use of force because the appropriate response may well be something quite different. And you really just want to end the very cyber activities that are going on.

I think the basic point is that, as a matter of law, the Article 51 of the Charter will apply. It will apply in cyberspace. It is not easy because of the indirect and direct consequences, because of what Doug said, it may or may not be successful. I certainly agree that it is difficult to think of examples that reach the threshold of an armed attack where physical destruction or death have not occurred. I think that is quite difficult, but rather than focusing on immediate physical effect, I think a more useful framework that we could use would be to focus on the reasonably foreseeable consequences of a particular cyber operation and the level of interference in state function.

On countermeasures, yes, that is an important consequence of finding an international wrong. They have their own limitations, of course, but they are an important consequence that states can explore.

Monica Hakimi

Okay. Just for viewers at home, when we speak of countermeasures, we generally refer to conduct that is otherwise unlawful but is permitted in response to an unlawful act by the other side. Here, the question is when may a state suspend its ordinary obligations in response to an unlawful cyberattack? There is, of course, another category of unfriendly conduct that a state might take in response to an attack. Retorsions are not otherwise prohibited and are always available to a state. So a victim state may presumably use retorsions in response to a cyberattack or otherwise.

But let us just focus on countermeasures. Let us assume that a cyberattack of some kind causes a harm that is prescribed by international law, and so a state has a right to respond with countermeasures as limited by international law. Ann, I would like to get your view on whether other states that are not directly affected by the cyberattack may also respond with countermeasures—whether there is what is known as a right to take collective countermeasures in response to an unlawful cyber act.

https://doi.org/10.1017/amp.2021.79 Published online by Cambridge University Press

Ann Väljataga

This is a particular aspect where Estonian President Kersti Kaljulaid made an unexpectedly revolutionary statement last May during the opening speech of CyCon. According to her, according to Estonia's official position, yes. States may respond in a collective manner to a cyberattack, and the argumentation for this very bold claim was mostly that it does not necessarily bring about escalation or need escalation, but to the contrary, it might lead to the use of milder measures to respond, because when a state that is under risk of cyberattack and does not lack the technical means, but at the same time is working in close alliance with other states, but the other states are not allowed to step in, then the state might, in fact, choose harsher avenues of response.

Secondly, there is the nature of the cyber domain and shared responsibility, just the very fact that one vulnerability of the territory of one sovereign nation state directly influences the overall structure. These arguments were chastised and praised to an equal extent, but still there are not many states that are coming up with bold statements. It is often criticized that it opens up new opportunities for opportunistic unnecessary aggression, but against these claims I would say that collective or not, countermeasures still have to be proportionate.

Monica Hakimi

Ann, I would like to pin you down, if I may. Let us be technical lawyers for a minute. If you take the position that collective countermeasures are in some circumstances lawful, they have to be proportionate. They must be intended to have a non-escalatory effect. How do you grapple with the Draft Articles on State Responsibility in this context? Do you say that collective countermeasures are generally lawful, and the suggestion in the Draft Articles on State Responsibility that they are only permissible when taken by a state that is specifically injured is wrong or dated? Or do you say that cyber conduct is, in some way, different so that the ordinary principles on countermeasures and the injured state criterion that the International Law Commission offered up do not apply in this context?

Ann Väljataga

Another question, which is more complicated, is exactly what kind of a cyberattack can be responded to in a collective manner? Is there such a thing as a violation obligation *erga omnes* of cyber sphere? The exact nature of a cyberattack that can be replied to in such a manner, this is something that, because of the lack of state practice, we cannot illustrate or we cannot offer any real-life examples, illustrative examples that would help to put this issue into context, unfortunately.

It is not a matter of whether there are some kind of cyberattacks that might constitute a universal threat. Probably, there are, but we are yet to figure out whether such attacks have occurred already and determine the criteria that we could use to decide whether a particular cyberattack qualifies as, say, use of force, but not an armed attack, and what kind of cyberattack could actually bring about collective response?

Monica Hakimi

Okay, great. I want to ask another question and then ask each of you to weigh in, and if you have thoughts about the countermeasures question, you are welcome to address it. The more general question that I want to ask starts with the understanding that there is a lot of uncertainty in the law that governs cyber, both at the broad, general prescription level and as applied in concrete

https://doi.org/10.1017/amp.2021.79 Published online by Cambridge University Press

cases. Even if we can agree, for example, that some cyber conduct might cross the armed attack threshold, it is hard to figure out exactly where that threshold is. There is quite a bit of uncertainty.

The question I have for the governmental lawyers who are actually advising clients on a regular basis in this space is, how do you lawyer in the face of that uncertainty, and how do you use international law to guide your clients in light of, Doug, something that you mentioned earlier, both the offensive and the defensive nature of this domain and what states are doing here? And for the nongovernmental lawyers, the question is, what prospects do you see for further clarification of the law? Do you think that is something that is realistically in view, or do you think in the near to medium term, we are likely to continue operating in a zone of uncertainty? Doug, I will start with you, and then we can just go Doug, Sue, Chuck, Zhixiong, Ann, and wrap it up.

Doug Wilson

Thanks, Monica. I will try to be brief. How do we approach this? I think what we try to do, as I said at the start, is look at cyber power in the round, understand the linkages and interaction between the domestic and international legal frameworks, which we are applying both at the same time to the same situations as will many other countries.

Cyber is not unusual in that sense. There are many areas of state conduct and international affairs in which you have to approach it in that way.

What I would say is that, certainly, over the last few years, there has been a lot more common understanding and common cause about the general principles and application of those principles than there was before. I think it is possible to overstate the uncertainty in this area, even recognizing that we want to see further discussion and alignment of how the law applies in the specific activity. What we are trying to achieve by that is both an ability to attract, as we are able to do in a whole host of areas, international alliances or calling out bad behavior, as I have seen a range of countries do in recent years, and also understand the rules applying to the projection of cyber power. Because we cannot have a situation for those countries that subscribe to an international rules-based system are unable to project that kind of cyber power in the defending forward way that Chuck mentioned, and that such offensive activity is confined to those countries that have no regard for the rule of law, at least in their covert actions.

What we are trying to do as international lawyers is like any other area, especially emerging areas over decades, understand the laws that apply, come to common understandings as to what activity is permitted and what is not, and then I think there will over the course of future years be room for progressive development and rule-making in this space when the time is right and when the countries can come together to do that in a meaningful and sensible way. Thanks.

Sue Robertson

Beautifully said, Doug. I agree with many of those sentiments, so thank you.

In quick time, I just want to consider "what do we do?" We start with fundamental first principles, and we go from there. And we have to understand the object and purpose of what the law is trying to do. One thing we have really tried hard to do where the law is less certain is to publicly express our view of where the legal interpretations lie, because we believe we have responsibility as states to do so, to explain state practice recognizing that state practice in this area is hard to describe at times. Often we are left more with describing *opinio juris*. But I think if states are not willing to do that, to fill that gap and describe their own bright lines, others will fill that gap for us and may take the law in a direction that we think is less useful. That is why we have been attempting to make public some of those legal views and through case studies as well. I know NATO has done this as well. I think the case studies are really a good example of trying to

https://doi.org/10.1017/amp.2021.79 Published online by Cambridge University Press

show the application of the basic principles of international law to hypothetical situations and to show that legal reasoning, how it can assist in defining international wrongs and promoting peaceful dispute resolution processes.

Charles Allen

Well, thank you for those comments. Actually, what Sue said leads right into what I wanted to say. Starting with first principles, understanding the object and purposes of what the law is trying to do, and especially where the law is less certain, states have a responsibility to express publicly their views on the law that applies. As we address these questions, we need to have a sense of both humility and pragmatism, and as Sue said, adhere to first principles. We need to keep in mind that balance is required, that the same rule of international law that we conclude authorizes the U.S. military to conduct a cyber operation can also legitimately be applied against the United States. We need to avoid opportunistic shifting of legal views and instead provide consistent advice, principled advice.

I would like to comment about some of the speeches I have referred to. I am happy that during the last administration, the Obama administration, a number of very useful and important speeches were given. Senior counsel got together and took up the challenge of explaining publicly and in as much detail as we could the bases for U.S. actions, including in counterterrorism operations and such specific areas as cyber. In this context, we have the Harold Koh speech in 2012, and the follow-on Brian Egan speech in 2016, which talked about elections interference—even before it became such a prominent issue. Then we followed up with some other speeches, and I am happy to say much the same has been done in this administration. Likewise, we in the United States appreciate what other countries are saying, such as in the UK attorney general's speech.

I appreciate and am intrigued by many of the things said today, including what Ann said about the Estonian statement on collective countermeasures.

I believe this process should continue. After Paul Ney's speech in March 2020, there were statements in support of the speech and some critiques, as one would expect. Although the pandemic has made things extremely difficult for all of us, I am sure that this good and healthy discourse including discussions like this one we have had today will serve us really well. I would emphasize particularly the opportunity to hear from states. Continued participation by states in the norm-creation process, even in the sense of non-binding norms, as in the continuing work of the UN Group of Governmental Experts, whose work since approximately 2010 has made a valuable contribution and continues. We should continue on this path, understanding that no one has a corner on the market of righteousness in these matters. We need to be open to each other, keep exploring, and keep listening to one another. Thank you.

Monica Hakimi

Wonderful. Zhixiong?

Zhixiong Huang

I think the application of international law in cyberspace is a useful first step toward rule of law in cyberspace, but with the international legal framework as applied in cyberspace is too general to provide the necessary legal certainty. That uncertainty needs to be addressed.

I see two possible approaches. One is to enhance discussion and dialogue among nations. I would like to mention the two ongoing processes within the UN, the UN Open-Ended Working Group (OEWG) and the new UN Group of Governmental Experts (GGE). For example, China

https://doi.org/10.1017/amp.2021.79 Published online by Cambridge University Press

in last September for the first time issued a position paper in the OEWG, at least partly relating to the application of international law in cyberspace, which is publicly available. That shows the discussion among states has generated encouraging progress.

The other is the possibility to supplement and to fill in the gaps in international law with soft law initiatives. This is what is already being done in reality. For example, in the 2015 UN GGE Report, we can see in paragraph 28(b) that states must comply with their obligations under international law to respect and protect human rights and fundamental freedoms. At the same time, the Report also made the view in paragraph 13(e) in the section on "norms, rules, and principles for the responsible behavior of States," that states, in ensuring the secure use of ICTs should respect the relevant Human Rights Council resolutions as well as the General Assembly resolutions to guarantee respect for right to privacy, right to freedom of expression, and other human rights.

It is like how the adoption of the Universal Declaration of Human Rights in 1948, which was non-binding at that time, elaborated on and clarified the human rights provisions in the UN Charter. I think this trend, the mutual reinforcing of soft law, the non-binding norms, and binding international law, will continue in the coming years.

Monica Hakimi

Thank you. Ann, I am going to ask you to wrap up for us with some final comments, if you have any, and then I will say thank you.

Ann Väljataga

As for the last question, just very quickly, as I am one of the panelists who has no experience with being a state legal adviser, I would like to thank everybody involved in fact-forming the state's opinion on cyber matters because recently, say during last two years, we have been reading and receiving interesting, relevant, on point, and strong writings expressing state opinions. We have Australia, the UK, the Netherlands, Estonia, and France expressing explicitly their positions on international law as applied to cyber operations. In addition to this, we are witnessing legal vocabulary, and legal-sounding statements or legally meaningful statements in national cybersecurity or cyber defense strategies more and more. For me, personally, this is even more an interesting and relevant read, and I feel it to be more significant to the emergence of international cyber law than some of the many soft law norms-based instruments. This is where I would like to show my appreciation to everybody in fact involved in creating this kind of state legal opinion.

Monica Hakimi

I think that expression of gratitude is a great place to end. I want to thank all of you for taking the time to meet with us today, and thanks to ASIL for having us. Thanks to our audiences who are still with us. I look forward to learning more about these topics from all of you as life progresses. To conclude, I will just clap on behalf of everyone in the room. Goodbye.

https://doi.org/10.1017/amp.2021.79 Published online by Cambridge University Press