Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace

by Przemysław Roguski

March 6, 2020

A large-scale cyber attack knocked out thousands of websites in the country of Georgia on October 28, 2019. The attack—and the chorus of state responses to it—provide an important window into the current status of international law in this domain and the politics of attributing cyber attacks to other governments. I argue that the Georgia attack shows the opportunity costs of states not firmly grounding their reactions in the language of international law.

The cyber attack on Georgia was launched against the websites and servers of governmental agencies, state bodies, courts, academia, NGOs, as well as commercial and private financial targets. Many of the affected websites were defaced, such as replaced with an image of the former president of Georgia, Mikhail Saakashvili accompanied by the text "I'll be back." The TV station Imedi was knocked offline and was unable to broadcast its signal, and another station's computers were reported to be damaged. Although the attack in itself was not very sophisticated, the scale of the incident was unprecedented and has created insecurity and confusion among the public and rendered certain governmental services inoperable for some time.

Nearly four months later, on February 20, 2020, Georgia, the United Kingdom, the United States, the European Union and many other States, in a series of generally coordinated statements, publicly attributed the cyber attack to the Main Center for Special Technologies (GTsST or "Unit 74455") of the Russian General Staff Main Intelligence Directorate (GRU), namely, the Russian military intelligence service. The unit is also known to operate under the names Sandworm, BlackEnergy Group or VoodooBear and is alleged to be responsible for, among other activities, the cyber attack on Ukraine's electricity grid in December 2015 and the NotPetya cyber attack in June 2017. Although none of the States presented the evidence upon which the attribution has been made against Russia for the Georgia attack, the United Kingdom assessed the correctness of its attribution as "almost certain" (95% + probability).

Assessment of the public attributions: light and shadow

The largely coordinated public attributions of the cyber attacks against Georgia are noteworthy for their scale: so far over 20 countries (all "Five Eyes" members, the European Union as a whole and many EU Member States individually, although not France or Germany) have issued statements on the matter. In previous instances, such as the December 2017 coordinated attribution to North Korea for the WannaCry cyber attack, or the October 2018 attribution to Russia for the World Anti-doping Agency hack, it was mainly the Five Eyes members (Australia, Canada, New Zealand, United Kingdom, United States) along with a few western partners which made their views public. The increased number of participants in the case of Georgia may point to the fact that more – especially European – States are willing to adopt public attributions as a foreign policy tool and have the technical capacity to do so. What's more, it shows that malicious actions in cyberspace are increasingly perceived as a problem requiring a coordinated and unified response of States sharing the same views about responsible behaviour in cyberspace. States' willingness to show solidarity may also stem from the fact that they too have been (in cases of Estonia or Ukraine) – or fear to become (in cases of Poland, Czech Republic, Latvia etc.) – targets of disruptive cyber attacks.

Nevertheless, the attributions are also striking for what they omit: namely a clear reference to a rule of international law the attributed cyber conduct allegedly breached. For instance, the statement by U.S. Secretary of State Mike Pompeo speaks only of how this action "contradicts Russia's attempts to claim it is a responsible actor in cyberspace and demonstrates a continuing pattern of reckless Russian GRU cyber operations against a number of countries." Similarly, the United Kingdom's statement refers to "an attempt to undermine Georgia's sovereignty," with Foreign Secretary Dominic Raab calling the "GRU's reckless and brazen campaign of cyber-attacks against Georgia, a sovereign and independent nation, … totally unacceptable." Some States, such as the Netherlands and New Zealand, refer to "norms of responsible behaviour in cyberspace" generally, while others, such as Australia, Canada and Latvia, also reference international law without however, pointing to a specific obligation. Only Georgia seems to be more concrete when speaking about the cyber attack as "infringing Georgia's sovereignty." Use of the terms "infringing … sovereignty" is more in the vein of international legal parlance than "undermining."

This overall lack of specificity, together with the absence of hard evidence establishing the GRU's responsibility for the cyber attack, blunts the impact – and possibly also the deterring effect – of the collective attributions. It consequently made it easier for Russia to dismiss the statements as "unsubstantiated and politically motivated." More importantly however, without clearly naming the rules of international law that Russia

violated, it is hard to engage Moscow's international responsibility and require it to cease its actions in a legally meaningful way. The statement put out by the Russian embassy in Australia put the finger on this problem, saying that "cyberspace … should be regulated through consensus and international law rather than 'rules' drafted and imposed by a handful of states." In this case it could therefore be argued that the United States and its allies have missed an opportunity to strengthen the international rules-based order in cyberspace by setting out in clear terms their view of which rules the October 2018 Russian cyber attack actually violated. Consensus-building over the applicable rules and norms in cyberspace can only work if there is clarity about the applicable rules and the circumstances that lead to a breach of those rules.

Did the cyber attacks breach Russia's international legal obligations to respect Georgia's sovereignty?

The reluctance to refer to specific rules of international law may stem from the fact that the legal qualification of cyber attacks which fall below the threshold of use of force and do not amount to an intervention into the internal affairs of a State is still not fully settled. According to some scholars, most notably the authors of the Tallinn Manual 2.0, such cyber attacks might violate the obligation to respect another State's sovereignty, which, in their view, also applies in cyberspace. Others hold the view that sovereignty is a principle of international law, rather than a rule and deny its applicability to cyberspace. The arguments of the "sovereignty as a rule" vs. "sovereignty as a principle" debate have been laid out in detail at *Just Security* before (for instance here, here, here and here) and I will not repeat them. I would like however to make three observations with respect to the sovereignty debate in context of the Russian cyber attack against Georgia.

First, if one adheres to the "sovereignty as a rule" position, then the cyber attacks would have apparently constituted a violation of sovereignty. According to the commentary to Rule 4 of Tallinn Manual 2.0, a cyber attack need not only produce physical damage or loss of functionality of the attacked systems to qualify as a violation of sovereignty. Rather, a violation also exists where "inherently governmental functions" such as the delivery of social services, the collection of taxes etc., are being interfered with. In the Georgian case, the cyber attack was, according to Georgian authorities, "launched against the websites, servers and other operating systems of the Administration of the President of Georgia, the courts, various municipal assemblies [and] state bodies, [as a result of which] the servers and operating systems of these organisations were significantly damaged, severely affecting their functionality." It seems, therefore, that there has been an interference

with inherently governmental functions. This assessment is even clearer if one applies the penetration-based approach proposed by France, whereby "any unauthorised penetration" of computer systems on the territory of a State "may constitute, at the least, a breach of sovereignty."

Secondly, in my view, the cyber attack against Georgia lays bare the weaknesses of the "sovereignty as a principle" approach. If sovereignty is merely a principle, rather than a rule of international law, there seems to be no rule of international law which Russia might have breached in this case. The cyber attack did not amount to a use of force as its scale and effects are not comparable to the use of kinetic force. What about the rule of non-intervention? , Affecting the functionality of governmental websites and servers, even if severe in effects, is not enough to constitute coercion on the free exercise of the sovereign will of a State, which would have been necessary to qualify the cyber attack as a prohibited intervention. For the proponents of the "sovereignty as a principle" approach, the only way to condemn Russia's actions seems therefore to be to invoke "rules of responsible State behaviour" in cyberspace, rather than international law. However, these norms, proposed by the U.N. Group of Governmental Experts in 2015, are only "recommendations for consideration by States" and of a non-binding character. What's more, should Georgia wish to react to the Russian cyber attack by taking more firm actions than a public statement of attribution – for instance by implementing countermeasures – such actions would be justified under international law only as a reaction to a previous breach of an international obligation.

Thirdly, the inadequacy of condemning cyber attacks solely on the basis of non-binding "rules of responsible behaviour in cyberspace" shines through in the statements made by certain States. Many of them refer both to international law and rules of responsible behaviour. The United Kingdom, for instance, described the cyber attacks as "an attempt to undermine Georgia's sovereignty" and Foreign Secretary Dominic Raab said that "[t]he Russian government has a clear choice: continue this aggressive pattern of behaviour against other countries, or become a responsible partner which respects international law." Given that the United Kingdom's official position, stated in May 2018 by then-Attorney General Jeremy Wright, QC, is that "there is no such rule [of territorial sovereignty in cyberspace] as a matter of current international law," one wonders which rule of international law – if not sovereignty – is Russia accused of disrespecting? It is not good for the global legal system regulating cyber and other activities to leave the answer to such a question ambiguous.

Is there growing momentum for the 'sovereignty as a rule' position?

While Foreign Secretary Raab's statement is not specific enough to be seen as a shift in the UK's position on sovereignty in cyberspace, it has to be noted that the United Kingdom is so far alone in (publicly) holding this view, while the number of proponents of the "sovereignty as a rule" position seems to be growing. Last week, Georgia and the Czech Republic (on Twitter) have held that attacks like the one on Georgia "are a clear violation of state sovereignty" and while deducing a State's position on whether sovereignty is a rule of international law applicable in cyberspace from such short statements should be approached with caution, it shows a growing awareness that cyber attacks may affect State sovereignty. Before that, Germany, the Netherlands and France have argued in more substantiated statements that cyber attacks may constitute a violation of sovereignty and thus entail the international responsibility of the State conducting the attack. With France and the Netherlands publishing their views on sovereignty in cyberspace after the U.K. position and now potentially Georgia and the Czech Republic joining in, there seems to be, therefore, a growing momentum for the "sovereignty as a rule" position.

It has to be noted that one prominent commentator, writing in Just Security, contended that "France did not assert that sovereignty constitutes a standalone primary norm of international law." He based this on the fact that the French document on "International Law Applicable to Cyber Operations" of September 2019 was published by the French Ministère des Armées and thus did not represent the official position of the French government but rather was "in the same vain as the DoD Law of War Manual." Furthermore, it was argued that the document "at no point [asserts] unequivocally that a violation of the principle of sovereignty constitutes a breach of an international obligation."

Respectfully, I disagree. As I have written elsewhere (and see also professor Mike Schmitt's analysis), the 2019 document forms the (provisional) culmination in the evolution of the French position on this matter and was preceded by several major strategy papers, as well as two major speeches by then-Minister of Defense Jean-Yves Le Drian. Already the 2018 "Strategic Review of Cyberdefense" (*Revue stratégique de cyberdéfense;* English summary) lays out (at p. 80) that cyber attacks may amount to a violation of sovereignty and thereby constitute an internationally wrongful act. This has been affirmed in the French response to UNGA Resolutions 73/27 and 73/266 (French version, English version). In sum, the September 2019 document represents the official view of the French government, rather than an opinion of only one governmental department.

In all these documents, France stresses that the production of effects on French territory by cyber means, or the penetration of French systems, may constitute a breach of sovereignty (an international legal delict, to be more exact). The Strategic Review of Cyberdefense makes clear that such a breach would be regarded as an internationally wrongful act. It states:

> "*Caractérisation comme aggression armée au sens de l'article 51 de la Charte des Nations-Unies [est] [p]robablement impossible: les actions correspondant à ces niveaux pourraient néanmois constituer d'autres faits internationaux illicites (intervention, violation de la souveraineté, usage de la force, etc.).*"
>
> "Characterising [level 0-4 cyber attacks] as armed attacks within the meaning of Article 51 of the UN Charter [is] probably impossible: actions corresponding to these levels could nevertheless constitute other internationally wrongful acts (intervention, violation of sovereignty, use of force, etc.)." (Just Security translation)

The French response to the UNGA Resolutions is also clear. It states:

> *The principle of sovereignty applies to cyber space. To this end, France reaffirms that it is exercising its sovereignty over information systems, persons and cyber activities in its territory, within the bounds of its obligations stemming from international law. *The unauthorized penetration of French systems or the production of effects in French territory via cyber means by a State entity, or non-state actors acting under the instructions or the control of a State, can constitute a violation of sovereignty.*

The statement's reference to non-state actors acting in a manner attributable to a state as well as the term "violation" clearly convey the understanding that such cyber operations would violate an international obligation on states.

Nothing else follows from the September 2019 document. It states:

*When carried out to the detriment of the rights of other States, [cyber] operations may breach international law. Depending on the extent of their intrusion or their effects, they may violate the principles of sovereignty, non-intervention or even the

prohibition of the threat or use of force. … In response to a cyberattack, France may consider diplomatic responses to certain incidents, counter-measures, or even coercive action by the armed forces if an attack constitutes armed aggression.

Which response mechanism to choose will depend on a political decision and the gravity of the cyber security incident (the *Strategic Review of Cyberdefense* employs a scale from 0 to 5, with 0 signifying an incident with negligible impact and 5 signifying an incident with extreme impact, possibly constituting an armed attack). So not only is the French position not "deliberately vague," as has been claimed. Rather, it is quite clear both on the elements of a breach of sovereignty, as well as on the responses, which include the full range of measures permitted under international law.

The correct view is therefore that France, together with Germany and the Netherlands, and possibly joined by Georgia and the Czech Republic, affirm the existence of a rule prohibiting the violation of another State's sovereignty in cyberspace.

Conclusion

Cases such as the Russian cyber attack against Georgia demonstrate that without a clear rule prohibiting the violation of a State's sovereignty in cyberspace, many cyber attacks falling below the threshold of use of force would not be regulated by international law. Under those circumstances, public attributions and calls on the responsible State to cease its actions would amount to nothing more than political condemnations, rather than legally significant invocations of the international legal responsibility of perpetrating States. Most importantly, lacking the ability to invoke a prior violation of an international obligation, States would not be authorized under international law to apply countermeasures. To strengthen the development of an international rules-based system applicable to cyberspace, States should, when making public attributions, clearly state the rules of international law which they view as having been violated and not shy away from affirming the existence of a rule of territorial sovereignty. When states stop short or leave their views ambiguous, it only encourages further malicious activities by aggressive states.

About the Author(s)

Przemysław Roguski

Dr. Przemysław Roguski is a Lecturer in Law at the Jagiellonian University in Kraków (Poland) and an expert on cybersecurity and international law at the Kościuszko Institute. Follow him on Twitter (@Roguski_P).