Reiss Center on Law and Security
NYU School of Law
JUST SECURITY

**What You Need to Know:**
**Unpacking the Law in Russia's War Against Ukraine**

# Genocide Determinations and Ukraine

**Todd Buchwald** | June 14, 2022

*Todd Buchwald is a member of the UN Committee Against Torture and teaches international law at George Washington University Law School. He previously served as the U.S. Ambassador for Global Criminal Justice at the U.S. Department of State. Before that, he served in a variety of capacities in the State Department's Office of the Legal Adviser across multiple administrations, including as the Assistant Legal Adviser for United Nations Affairs and the Assistant Legal Adviser for Political-Military Affairs. He was the inaugural Tom A. Bernstein Genocide Prevention Fellow at the Simon-Skjodt Center for the Prevention of Genocide of the U.S. Holocaust Memorial Museum, and co-chaired (with Beth van Schaack) the American Society of International Law Task Force that produced the report on Policy Options for U.S. Engagement with the International Criminal Court.*

### To begin, how does the U.S. government ordinarily make decisions whether to say, or not to say, that genocide has occurred in a particular situation?

There is no formal policy governing how this is done but a *de facto* process has emerged over time. Traditionally, decisions have been made at very senior levels, typically by the Secretary of State, based on information that is developed, marshaled and analyzed by relevant State Department bureaus, including the relevant regional bureau, the Office of Global Criminal Justice, Bureau of Intelligence and Research and the Office of the Legal Adviser. In at least some cases, the Department has supplemented the available information with reports from investigators it has commissioned to conduct interviews with displaced victims to better understand the situation. However, this de facto process appears not to have happened in connection with President Biden's statement that genocide was being committed in Ukraine.

### Was the president correct when he declared that genocide was being committed in Ukraine?

In fairness, Biden said at the time that this was simply his view and he would "let the lawyers decide internationally whether or not it qualifies."

That said, the answer to the underlying question depends as much on what one thinks constitutes "genocide" as what one thinks has happened on the ground in Ukraine. On the one hand, colloquial understandings of the term are based largely on subjective factors—for example, the extent to which the conduct in question evokes the crimes committed by the Nazis, feels as if it stands at the pinnacle of evil, or warrants an obligation by the international community to intercede. The sheer number of victims is often highlighted and there is a general sense that genocide includes an eliminationist element—that the perpetrators aim to eliminate the relevant group—but no agreed understanding of what "eliminate the relevant group" means.

Such colloquial understandings of genocide are not "wrong," but they do not match the definition traditionally applied by international lawyers, or the U.S. State Department, who instead use the definition in the 1948 Genocide Convention as their point of departure. That definition has gained

only more stature over time, and is included virtually verbatim in such instruments as the Statutes of the *ad hoc* Tribunals for Former Yugoslavia and Rwanda (ICTY and ICTR) and the Rome Statute of the International Criminal Court.

**"[T]he answer to the underlying question depends as much on what one thinks constitutes 'genocide' as what one thinks has happened on the ground in Ukraine."**

At the same time, although the Convention's definition of genocide is widely accepted, it is not altogether clear. For Russian conduct to come within its terms, three tests must be met. First, a perpetrator must commit one of the predicate acts that are enumerated in the definition, such as killing members of any of the kinds of groups listed in the definition. As to this test, the conclusion that there have been "killings" in Ukraine is self-evident.

Second, the target must be a "national, ethnical, racial or religious" group. The drafters of the Convention thus decided that the intent to destroy numerous other types of groups—e.g., political, economic or linguistic groups—would not qualify. Of the types of groups that the Convention does cover, the most relevant here are "national" or "ethnical." Russia might well challenge the conclusion that Ukrainians qualify—e.g., it might argue that "national group" refers to national minorities in the sense of the treaties that followed World War I rather than persons who share citizenship. But President Putin himself appears to refer to Ukrainians in a way—e.g., speaking about them in the same breath as "Tatars, Jews and Byelorussians"—that would make such a challenge difficult.

Third, the killings (or other predicate acts) must be committed with a specific intent "to destroy, in whole or in part, [the relevant group], as such." This third test is the most difficult, and has often been a source of debate and misunderstanding.

### What are the key interpretive issues under this third test?

There is a fuller discussion in the report that Adam Keith and I produced for the United States Holocaust Museum. In the first place, the fact that the intent must be to destroy the group "as such" means that the targets must be being attacked *because* they are members of the group—e.g., the Ukrainians are being attacked *because* they are Ukrainians—as opposed to being attacked because they stand in the way of (for example) military conquest. This is why military campaigns aimed at subjugating foreign nations, awful as they are, generally are not by themselves talked about as genocide.

In addition to the interpretation of "as such," key issues include—

- What does the Convention mean when it says that, to constitute genocide, the killings must be committed with the intent to "destroy" the relevant group?
- What does the Convention mean when it speaks about destroying the relevant group "in part"?
- How clear should the evidence about intent be in order to conclude that genocide has been committed?

### Let's address these questions in turn. First, what does "destroy" mean?

The key question here is whether—to fall within the Convention's definition—the perpetrator must intend to destroy the members of the group in a physical or biological sense, or whether it is sufficient to destroy the group in the sense of preventing its members from continuing to function as a group.

For its part, the International Court of Justice (ICJ) has said that the intent must be to destroy the group in a physical or biological sense, and that this interpretation is based on the Convention's negotiating history. The concept of "cultural genocide"—destroying the ability of the group to continue functioning as a group—was clearly reflected in Raphael Lemkin's original conception of "genocide." It was similarly reflected in the so-called Ad Hoc Committee draft of what eventually became the Genocide Convention, which contained an entire bracketed section—entitled "Cultural Genocide"—under which acts such as prohibiting use of a group's language or destroying its places of worship would

qualify as genocide if committed with the requisite intent to destroy the group. But the section on cultural genocide did not survive, and the international courts have read its deletion as evidence that only destruction of a group in a physical or biological sense suffices. (See paragraph 135 et seq of the ICJ's 2015 Judgment in Croatia v Serbia.) This has also been the understanding of the U.S. State Department when it assesses whether genocide has occurred in a country.

It is worth noting that, while this conclusion is widely held, it is not beyond debate. For example, one ICTY Judge reasoned that although the drafters had deleted acts of cultural genocide (e.g., prohibiting use of a group's language or destroying their places of worship) from the list of predicate acts that could qualify, it does not follow that they intended to exclude the commission of acts that were retained on the list (e.g., killing members of the group) if committed for the purpose of destroying the ability of the group to function as a group. (See paragraph 45 et seq of Judge Shahabuddeen's partial dissent in Prosecutor v Krstic.) In other words, the fact that widespread efforts to prevent use of the language or to destroy places of worship with the goal of destroying the group's ability to function as a group would not qualify as genocide does not necessarily mean that widespread killing of its members with that same goal would not qualify.

**"[T]he fact that the intent must be to destroy the group 'as such' means that the targets must be being attacked *because* they are members of the group—e.g., the Ukrainians are being attacked because they are Ukrainians—as opposed to being attacked *because* they stand in the way of (for example) military conquest."**

The approach suggested by Judge Shahabuddeen's partial dissent would leave more scope for a finding of genocide in Ukraine today. Under it, the "destroy" part of the definition could be satisfied if it were established that the Russian campaign was directed toward destroying the ability of Ukrainians to continue existing as a national or ethnical group. That said, a conclusion based on a premise that the ICJ had rejected could risk criticism that the decision-making had been politicized.

**Second, assuming the requirement to "destroy" entails physical or biological destruction, what does it mean to destroy a group "in part"? How large a "part" of the overall group must the perpetrator intend to destroy in order to fall within the Convention's definition of genocide?**

There is no clear answer to this question. In the U.S. ratification process, the Senate adopted an Understanding that the perpetrator must intend to destroy a "*substantial* part" of the wider group. U.S. legislation implementing the Convention into domestic law provides that, to qualify as substantial, the part must be "of such numerical significance that the destruction or loss of that part would cause the destruction of the group as a viable entity within the nation of which such group is a part." For its part, the ICJ has similarly said that "the part targeted must be significant enough to have an impact on the group as a whole," while also saying that the requirement of substantiality "is demanded by the very nature of the crime of genocide." (*See* paragraph 198 of the Judgment in Bosnia and Herzegovina v Serbia and Montenegro.)

There is some tension between these approaches to "substantiality" and the idea that the Convention is concerned only with the physical or biological destruction of the members of the group. They would appear to leave greater scope for a finding of genocide if it could be established that the perpetrator intended to kill a sufficient number of persons so as to prevent "Ukrainians" as a group from continuing to function as such as an objective of a policy of "de-Ukrainization."

Importantly, international courts have found that considerations beyond numerical size may also be relevant in assessing substantiality. For example, in the context of Srebrenica, the ICTY concluded that even though the Bosnian Muslims in Srebrenica formed only a relatively small percentage of the total number of Bosnian Muslims

in the country, it was appropriate to consider a series of qualitative factors in assessing whether their slaughter constituted genocide. These factors included the prominence of the Bosnian Muslims of Srebrenica within the overall group of Muslims in Bosnia, whether the Bosnian Muslims of Srebrenica were emblematic of the group as a whole, whether their survival was essential to the survival of the wider group, and the area of the perpetrator's activity and control. In the specific case of Srebrenica, the Tribunal looked to what it saw as the immense strategic importance of the area to the perpetrators, its prominence in the eyes of the international community, the fact that it had been declared a safe area by the United Nations Security Council, the example its vulnerability and defenselessness would serve to other Bosnian Muslims, and the fact that the geographic area of the perpetrators' operations was limited. (See paragraphs 12-16 of *Prosecutor v Krstić*.)

**"Importantly, international courts have found that considerations beyond numerical size may also be relevant in assessing substantiality ... it is possible to imagine a prosecutor arguing that the perpetrators intended to make an example of the vulnerability and defenselessness of the Ukrainian population in Mariupol as part of a plan aimed at the destruction of Ukrainians as a national or ethnical group."**

Could one apply a similar approach in analyzing events in Mariupol, Bucha or elsewhere? The mix of factors identified by the ICTY does not lend itself to a clear, easily applied legal test, and any factual assessment would need to account for intelligence and other information that is not publicly available. That said, it is possible to imagine a prosecutor arguing that the perpetrators intended to make an example of the vulnerability and defenselessness of the Ukrainian population in Mariupol as part of a plan aimed at the destruction of Ukrainians as a national or ethnical group.

### Third, how clear must the evidence be that the intent and other criteria have been satisfied in order to justify a determination that genocide has occurred?

Again there is no definitive answer, but at least three considerations warrant mention.

First, it is widely accepted internationally that the perpetrator would need to have "specific intent." From the perspective of the United States, this is reflected in both the Senate's resolution of advice and consent and the U.S. legislation implementing its obligations in domestic law. Knowing that the destruction of the group is likely is not the same as *specifically intending* to cause it. A state accused of genocide might well argue that its conduct was part of a military strategy simply to overrun the enemy, as opposed to a specific intent to destroy a group, and that even if the strategy included the illegal targeting of civilians, that would not by itself overcome this line of defense. In some cases (as with the Nazis), the perpetrators are open about their objectives, but in other cases, the fact that the definition requires specific intent can complicate the ability to draw the necessary conclusions.

The second consideration involves the burden of proof. At least at times, the courts have set the bar quite high in terms of how clear the evidence must be before they will infer that the conduct was carried out with the requisite genocidal intent. For example, the ICJ said in the *Croatia v Serbia* case that it would infer genocidal intent only where the evidence is "fully conclusive" and where "this is the only inference that could reasonably be drawn from the acts in question." (See paragraphs 143-148 of *Croatia v Serbia* and paragraph 373 of *Bosnia and Herzegovina v Serbia and Montenegro*.) Particularly in combination with the difficulty in establishing specific intent, this high burden of proof presents a formidable obstacle. To be sure, it does not necessarily follow that the United States or other states should apply the same standard in their own assessments, but this does reflect some sense that a finding of genocide is ordinarily viewed as exceptional and should be subject to a high burden of proof.

The third consideration involves the fact that different actors may be acting for different purposes. In any actual criminal proceeding, the particular defendant's individual circumstances would have to be examined with precision, including on questions of whether he or she acted with the requisite intent, or whether the circumstances were such that the genocidal intent of other actors should be imputed to the defendant. A simple statement that genocide has been committed in a country does not necessarily reveal whether it is senior leaders or local actors who are thought to be criminally responsible.

### What have other states said about whether Russian actions constitute genocide?

Most States do not typically make public statements about whether genocide has been committed in a country, though there are exceptions. For example, the U.K. has periodically made statements that such determinations are a matter for competent courts, but it nevertheless made statements regarding genocide by ISIS. States have been relatively forthcoming in making such statements about Ukraine and *Just Security* recently published an excellent survey by Elizabeth Whatcott. The statements are not easy to summarize. Many are from parliamentary sources that, in general diplomatic practice, would not be taken as a formal indication of a state's views. Of those made by executive officials, there is a mix. Some say flatly that genocide has been committed but do not specify the interpretation of the definition that they applied in reaching that conclusion; others—like the statement by Polish President Duda – are relatively specific and may have been framed with an eye on the definition in the Convention. Some of the statements talk about growing indications of the existence of evidence of genocide, without actually concluding that there has been genocide, or walk up to the line by suggesting that there are precursors or hallmarks of genocide. Some, like the statement by French President Macron, specifically avoid use of the word genocide, perhaps with an eye on leaving political space for an eventual rapprochement with Russia. Finally, some of the statements – like Biden's – are framed as reflecting the speaker's opinion, and not necessarily a formal view by the state of which he is the leader.

### Could international courts eventually decide the issue?

Yes, they could. The International Criminal Court (ICC) clearly has criminal jurisdiction over individuals who commit genocide in Ukraine. Interestingly, the ICC Prosecutor's announcement in late February that he would pursue an investigation of crimes in Ukraine said only that there was sufficient evidence to pursue charges of war crimes and crimes against humanity, but genocide was thereafter mentioned in both the formal referral to the Prosecutor submitted by 39 states and the Prosecutor's announcement to formally open an investigation on Mar. 2.

Meanwhile, the ICJ could address the issue of Russia's responsibility for genocide under Article IX of the Convention, which allows any Genocide Convention party to bring a dispute against any other party relating to the interpretation, application or fulfillment of the Convention. The United States could not bring such a case because it took a reservation to Article IX when it joined the Convention, but Ukraine or any other Genocide Convention party that has accepted Article IX could do so. For example, there is an ongoing case brought against Myanmar by Gambia, a state that many people would not routinely consider as having a direct interest, but the theory is that all parties owe obligations under the Convention to all other parties.

To this point, Ukraine has pursued a different strategy and brought an ICJ case based on Russia's wrongful claim that genocide by the Ukrainians legally justified Russian invasion. The Court has not yet addressed the merits of the claim, but very notably—by a 13-2 vote—issued an order that Russia suspend its military operations in the interim.

### Would a conclusion that Russian actions constitute or may constitute genocide trigger significant legal obligations for the United States or other states?

The U.S. government's answer to this question would be no. Parties have several specific obligations under the Genocide Convention—e.g., to enact the necessary domestic law to implement their obligations, to try persons charged with committing genocide in their countries, and to grant extradition requests in accordance with their laws and treaties in

force. But the United States has either already implemented these obligations or could easily do so if the situation arose.

More controversial is the scope of the obligation to "prevent and punish" genocide under Article 1 of the Convention. The United States has rejected arguments that this entails an obligation to prevent genocide in areas outside its territory, as stated for example in a 2004 memorandum prepared in connection with Secretary of State Colin Powell's eventual decision to state publicly that genocide had occurred in Darfur.

The ICJ has been more forward-leaning, saying that a state incurs liability if it has "manifestly failed to take all measures to prevent genocide which were within its power, and which might have contributed to preventing the genocide," though it noted that the capacity to influence events "varies greatly from one State to another." Read literally, this language could be understood to require military intervention—at least in cases where military intervention would otherwise be lawful and within the capacity of a state to undertake. But the sweeping language is likely a product of the particular circumstances regarding the broad influence that Belgrade at the time had over the Bosnian Serb perpetrators, and it seems doubtful that the Court would consider the broad array of support already being provided by the United States and others to Ukraine as insufficient to meet any such obligation that might exist.

In practice, different states will inevitably assert very different conceptions of what should be done to prevent or stop genocide in a given situation. For example, one state might argue that it is essential to terminate purchases of oil and natural gas, another might argue that such sanctions will only exacerbate the situation, and yet another might argue that purchases should be reduced but not terminated because the effect of termination on its economy would be too severe.

Importantly, the ICJ has said that a State's obligation to prevent does not depend on genocide having already occurred, but instead arises "at the instant that the State learns of, or should normally have learned of, the existence of a serious risk that genocide will be committed." (See paragraph 431 of Bosnia v Serbia.) This is in keeping with the idea that a key goal of the Convention is to *prevent* genocide. From this perspective, the question whether genocide has already occurred is too narrow, and it is at least equally important to focus on the level of risk of genocidal acts (or other atrocities), or whether eliminationist rhetoric or a campaign of vilification – *e.g*, about "de-nazification"—is contributing to a climate in which the risk of such atrocities increases.

### Even if there is no legal obligation to act, would such a conclusion trigger political or moral responsibilities for action by the United States?

This is a more complicated question. In the "Responsibility to Protect" principles adopted at the 2005 U.N. World Summit, states indeed agreed that the international community has a responsibility to use appropriate means to protect populations from genocide, but the text applies equally to war crimes, ethnic cleansing, and crimes against humanity. In this sense, the responsibility would be no greater or less in the context of genocide than in the context of these other crimes.

That said, the question of political and moral responsibility is complicated. A finding that genocide has occurred is widely perceived as carrying a special stigma, and as entailing an imperative to treat the conduct in question as the worst of the worst. It can often increase expectations of a robust response, galvanize political pressures to act, and frame the kind of responses and policies that the United States and other states would have the political space to pursue in the period going forward. The extent to which that is true in connection with Ukraine is unclear, as the response of western countries has been robust, even if short of direct military intervention.

At the end of the day, my view is that the U.S. government should draw conclusions based on its best assessment of the facts and the law, not colored by these other considerations; should straightforwardly explain its conclusions—and the policies it plans to pursue in light of those conclusions—to the American people and the international community; and should be prepared to apply the legal tests it applies in Ukraine consistently as other situations arise in the future.

# Russian Threats and Cybersecurity

**Beth George** | May 13, 2022

*Beth George is a Non-Resident Senior Fellow at the Reiss Center on Law and Security at NYU School of Law. She is a partner in the Silicon Valley Office of Freshfields Bruckhaus Deringer, where she leads the strategic risk and crisis management practice. Previously, she was a partner in the San Francisco office of Wilson Sonsini Goodrich & Rosati, where she led the firm's cybersecurity team. Beth served as Acting General Counsel of the Department of Defense in the Biden-Harris Administration. For her work, she was awarded the Department of Defense Medal for Distinguished Public Service, the highest honor the Department of Defense awards to civilians. Previously, Beth served as the Deputy General Counsel at the Department of Defense, as an Associate Counsel in the Office of the White House Counsel, and in various roles at the National Security Division of the Department of Justice.*

**Should we expect to see an increase in Russian cyber-attacks against the United States and other countries providing support to Ukraine as the crisis draws on? If so, what kinds of attacks would you predict we'll see, and do you think potential targets—particularly private companies—are sufficiently prepared?**

Since the earliest days of the Russian invasion of Ukraine, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has been issuing prominent warnings about the potential for an increase in Russian attacks against U.S. companies. They launched a campaign called "Shields Up" to provide warning and guidance to companies regarding potential Russian threats.

Interestingly, in the private sector, what we noticed around the time of the Russian invasion was a decrease in attacks that cybersecurity professionals generally attributed to Russian state-sponsored and state-affiliated hacking organizations, particularly regarding ransomware. Last fall, ransomware attacks appeared to be at their highest, with attacks against private companies happening on a routine basis, although many of the attacks were not existential for the company involved or didn't compromise major systems. (Anecdotally, in October 2021, multiple forensic companies I work with reported that they were at capacity for ransomware attacks and were unable to take on additional clients.) But by the time of the invasion, ransomware attacks had significantly dropped off, and those of us who work in the private cybersecurity sector remarked quietly among ourselves that it was disconcertingly quiet. It is unclear—at least based on publicly available information—whether this is related to Russian state-sponsored and state-affiliated hackers focusing their efforts on the war in Ukraine or if there has been some other type of disruption in their operations, perhaps due to efforts by the U.S. government to address ransomware gangs.

Regardless of how quiet it has generally been for the U.S. private sector in the past few months, Russia is clearly not out of the hacking game. Earlier this week, the U.S. and U.K. governments formally attributed an attack against ViaSat – a private internet satellite company—to the Russian government. In that case, the attack appeared largely intended to disrupt Ukrainian military activity, but it has secondary effects in several countries including, for

example, disabling remote access to thousands of German windmills that relied on the same technology.

As to whether private companies are sufficiently prepared for Russian cyber operations, the reality is that it is incredibly difficult for companies to pivot quickly to protect themselves from sophisticated state sponsored attacks. Building cybersecurity controls is a multi-year, and, in some cases, multi-million dollar investment. For companies that have underinvested in cybersecurity for years, getting basic controls in place to prevent or mitigate an attack is not something that can be done in a matter of days or weeks. That said, CISA is doing an excellent job of putting out information about known, exploited vulnerabilities putting out industry-specific and actionable threat intelligence. All companies would be well-advised to review CISA's public guidance and digest it into their cyber risk management processes.

**"[T]he reality is that it is incredibly difficult for companies to pivot quickly to protect themselves from sophisticated state sponsored attacks. Building cybersecurity controls is a multi-year, and, in some cases, multi-million dollar investment."**

### How serious are the potential threats to critical infrastructure in the United States from hostile cyber operations, and do you anticipate Russia targeting U.S. critical infrastructure?

There have been efforts across multiple administrations to raise awareness of cybersecurity threats to critical infrastructure, to share threat information with companies that own or operate critical infrastructure, and to improve private-public partnerships to further harden and protect these companies. Most recently, on Mar. 15, 2022, President Biden signed into law the *Cyber Incident Reporting for Critical Infrastructure Act of 2022* (within the Consolidated Appropriations Act), which will require entities determined to be critical infrastructure to report substantial cyber incidents within 72 hours and ransomware payments within 24 hours to CISA. But it's unlikely that it will have an impact any time soon—the statute allows the CISA director until September 2025 to establish implementing regulations. And because passage of the bill was strongly criticized by the Department of Justice and the FBI, there could be significant interagency fighting about the scope and content of the proposed rulemaking.

Perhaps more importantly, in June 2021, after the Colonial Pipeline ransomware attacks, Biden warned Russian President Putin that 16 critical infrastructure sectors should be off-limits from cyberattacks. Although it is not clear what the Biden administration has planned or specifically warned in the event of a critical infrastructure attack attributed to Russia, the presidential notice clearly raises the stakes for Russia: Putin must certainly expect that such attacks will have a significant response from the United States. In that warning, however, the administration took pains to differentiate between "destructive" hacks and "conventional digital espionage operations carried out by intelligence agencies worldwide."

In March of this year, Deputy National Security Advisor Anne Neuberger issued a public warning that the U.S. government is observing "threat intelligence that the Russian government is exploring options for potential cyberattacks on critical infrastructure in the United States." One can imagine that what the United States is observing is Russia conducting the very espionage activities that the United States was careful to distinguish as not off limits, but whether the Kremlin decides to exploit any vulnerabilities it has found or accesses it has established is what matters.

Regardless of Biden's warning, Putin certainly understands that there is a big difference between hacking private email accounts of administration officials and dumping the emails for an embarrassment campaign, compared to an attack that impacts water, electricity, or communications systems in the United States. Russia will always want the option to disable the critical infrastructure in the United States—much the same way other countries proactively seek to understand weaknesses in their adversaries' defenses. But I would be surprised if Putin were to take action against U.S. critical infrastructure because of the potential for it to result in significant escalation, whether of the conflict in Ukraine or more generally.

So despite the necessary focus on preparing for critical infrastructure cyberattacks, I would be more concerned about attacks on private companies or further disinformation campaigns. For companies that have made a noisy exit from Russia, Putin may wish to exact revenge or seek to embarrass them, not unlike North Korea's attack on Sony. For the Biden administration and the country, the November elections will be critical, and Russia has spent years honing its disinformation activities around U.S. elections. Seeking to further punish Democrats for their support of Ukraine through electoral losses would be an easy tool in Putin's toolbox, for which the response from the United States is highly unlikely to be as severe (or as bipartisan) as a response for an attack on critical infrastructure.

**You have served in several high-level legal positions in the U.S. government, in two administrations, including most recently as Acting General Counsel of the Department of Defense at the start of the Biden administration. When the U.S. government conducts cyber operations, how do the lawyers for the departments or agencies involved think about evaluating the legality of the proposed operation? How much technical expertise is required?**

The U.S. government has a deep bench of lawyers who have been thinking about these issues for a long time. Retaining that crucial, long-term memory and experience that exists in the civil service is incredibly important; and, under the current administration, it is complemented by a tech-savvy and seasoned political appointee team.

It is my experience that the vast majority of the lawyers in this area do not necessarily have technical backgrounds. Although having technological knowhow certainly helps, it is arguably far more important to have honed legal skills, including the ability to develop a full factual understanding of the scenario at issue. Often, as is the case in many areas of law, your clients provide you only with the facts that they think you need, and perhaps not the entire picture (usually in an effort to be efficient with your time or because they may not have sufficient understanding of the law to appreciate what other facts truly matter).

One of the key issues in applying law to cyber operations is grappling with the effects, both intended and foreseeable-but-unintended. Understanding that a particular activity doesn't start or end with the 1s and 0s being transmitted across the wire is a must; and it is crucial to have enough experience to ask the probing, and sometimes iterative, questions needed to evaluate fully what effects a particular operation is intended to have, or could unintentionally produce. There can be challenges in what can get lost in translation between the policy and legal worlds—for example, a client's use of the word "metadata" cannot be assumed to equal "noncontent" information under the Fourth Amendment. In the case of a complex cyber operation, it's imperative to ask enough questions to determine whether an activity is likely to merely affect one small portion of complicated machinery, for example, or could have follow-on effects. And in some cases, it's incumbent upon the lawyers to push back on clients when the operational uncertainty is too great; when it's not possible to fully understand the range of potential impacts of a cyber operation, it may not be possible to ascertain its legality. Simply wishing for the best possible outcome is not an appropriate course of action.

**"Understanding that a particular activity doesn't start or end with the 1s and 0s being transmitted across the wire is a must; and it is crucial to have enough experience to ask the probing, and sometimes iterative, questions needed to evaluate fully what effects a particular operation is intended to have, or could unintentionally produce."**

But all of these things are true for non-cyber operations as well. Whether it's lawyering traditional kinetic use of force, or merely delving into an area of a complex litigation regarding an intellectual property or financial dispute, basic lawyering skills are about understanding your clients, the language that they use, how to communicate with them, and how to get the facts you need to best advise them. These skills translate across subject matter.