doi:10.1017/amp.2025.7

CYBERWAR STRATEGIES AND ICC IMPLICATIONS IN THE AGE OF AI

This panel was convened at 10:30 a.m. on Friday April 5, 2024 by its moderator, Laurie Blank, who introduced the panelists: Charles C. Jalloh, François Delerue, and Sandra Hodgkinson.

Introductory Remarks by Michael Kelly

My name is Michael Kelly. I am on the organizing committee for ASIL and organized this panel specifically. Welcome to the roundtable where we will be discussing cyber weapons and the age of artificial intelligence (AI) and implications for the International Criminal Court (ICC). When you are a kid and you are wrestling with something that is challenging, you might recall your teachers telling you, "It is not rocket science or it is not brain surgery." In our scenario, cyber weapons is rocket science and AI is brain surgery. You are literally inserting a new brain into the rocket.

Luckily for us, our moderator today is both a rocket scientist and a brain surgeon. Laurie Blank is Special Counsel to the General Counsel at the Department of Defense, where she is doing amazing work for the U.S. government. Her academic home is Emory University School of Law, where she stood up and runs an amazing international humanitarian law (IHL) clinic, one of the first in the country to really break new ground in this area.

I will leave it to Laurie to run the panel and introduce the rest of our panelists. Thank you.

Remarks by Laurie Blank

Great, thank you. Good morning, everyone. Welcome to "Cyberwar Strategies and ICC Implications in an Age of AI." We are going to have a roundtable conversation. I am going to ask questions of our esteemed panelists after I introduce them, and we will keep going through a conversation and then leave plenty of time for questions from you all.

Let me also note, since I am currently at the Department of Defense, that I am here moderating and participating in my personal capacity, and none of what I say represents the view of anybody, the U.S. government, the Department of Defense, the military, probably even my own view.

Let me tell you briefly about our great panelists. Starting all the way on my left, we have Sandy Hodgkinson, who is currently Senior Vice President for Strategy, Sustainability, and Corporate Development at Leonardo DRS, an aerospace and defense company. Sandy had a really extraordinary career in the U.S. government, achieving the rank of Senior Executive Service, SES, in the U.S. government, including a number of really fascinating roles, Chief of Staff to the Deputy Assistant Secretary of Defense, Deputy to the Ambassador-at-Large for War Crimes Issues, Director for International Justice at the National Security Council, and Senior Advisor to the Coalition Provisional Authority in Baghdad. She also spent six years on active duty and fifteen years in the reserves in the U.S. Navy JAG Corps, retiring at the rank of Captain.

Immediately to my left is Charles Jalloh, who is currently the Kleh Distinguished Visiting Professor of International Law at Boston University Law School for this 2023–2024 academic year. He is the founding Executive Director of the Center for International Law and Policy in Africa, based in Freetown, Sierra Leone. He is serving his second term as a member of the International Law Commission, where he is the Special Rapporteur for the topic Subsidiary Means for the Determination of Rules of International Law. He has served as a Fulbright Distinguished Chair of Public International Law at Lund University in Sweden and currently chairs Canada's Independent International Panel on Arbitrary Detention in State-to-State Relations. I think our panelists win the award for the longest titled things that I have to read out. So I apologize for reading from my notes, but I do not want to get any of it wrong.

And then in the middle, last but not least, François Delerue, who is Assistant Professor of International Law at IE University, a member of the Jean Monnet Centre of Excellence for Law and Automation—this is the best name—also called "Lawtomation." I think we can finish the whole discussion right there after that, because that is just phenomenal. His recent book, "Cyber Operations and International Law," won the 2021 Book Prize of the European Society for International Law.

We have a wonderful set of panelists to lead us through this conversation today. I want to set the stage in about a minute. Let me share with you some descriptions of cyber and AI, including in the context of the conflict in Ukraine and other recent conflicts, just a quick description that sets the stage for what we are going to talk about. These are just from reports, news reports, and other things.

We see frequent use of drones and loitering munitions by both sides, offering AI-enhanced autonomous capabilities in flight, targeting, and firing. Both sides in that conflict have deployed autonomous ships, undersea drones for mine hunting, and uncrewed ground vehicles. We are starting to see the extensive use of AI in systems that integrate target and object recognition with satellite imagery, particularly and comprehensively in geospatial intelligence, including geolocating and analyzing open source data like social media photos in geopolitically sensitive locations.

We see parties to conflict analyzing vast amounts of data to produce battlefield intelligence regarding the party's tactics and strategies, using AI capabilities for that. And we also see the spread of misinformation and the use of deepfakes as part of information warfare.

Then I want to share four different terms that I have seen used to describe what we are starting to see and what is coming down the pike in this area. I have seen some describe this as "hyper-war," and I am going to read in quotes here, "a type of conflict and competition so automated that it would collapse the decision-action loop"—I think we know the Observe Orient Decide Act (OODA) loop—"eventually minimizing human control over most decisions" or "algorithmic warfare" in which autonomous systems and weapons independently start selecting their course of action based on the situation in which they find themselves." It has also been called "mosaic warfare," a more tactical term that combines conventional platforms with uncrewed systems to achieve battlefield advantages. The last I have seen is called "software-defined warfare," part of a vision in which software will be the crucial part of the defense architecture needed for next-generation warfighting systems.

I am going to turn to our panelists to set the stage for us. I am going to toss to each of you a question that will give us an introduction to some of this fascinating area, and then we will build from there.

Sandy, let me start with you. Building on this background, can you talk a little bit more about how cyber warfare, cyber operations, are changing on the battlefield as a result of AI and how the U.S. military and allied forces are prepared and preparing to meet these challenges?

Remarks by Sandra Hodgkinson

Thank you so much. Laurie just artfully threw out some fun terms. AI is in just about every single thing we do. I am in the defense industry now. Anything someone wants to sell or buy has to have AI right in front of it. It is all AI-enabled, AI-facilitated. It is a term of art that is being used a lot. But there are so many different applications, as you mentioned, from just the beginning description, everything from the unmanned weapons to battle networks to generative AI like ChatGPT to cybersecurity, logistics. It is everywhere in everything that the Department of Defense (DoD) and the U.S. military and foreign militaries are doing right now. These terms are coming up, and so trying to parse first what it is that is useful for the military commander on the battlefield, how it can enable a military strategic advantage for the United States, which first and foremost is what we try to do, is win wars and fight wars, and then to try to untangle that from the risks that it poses and try to put then international law and responsibility on top of it so that it is used in the way it is intended to be, which is to legally fight and pursue and prosecute wars to the extent that you can as a nation.

I know at its best, we will hear, whether it is Kat Hicks or DoD and all the variety of comments they have been making on this—about trying to make sure that we are enabling a battlefield advantage and that we are using AI in a way that helps us to win wars, and so the ways that you can do that involve a better, more accurate flow of information on the battlefield. For all of us who served in the military, there is nothing more important than getting good, actionable information in a timely manner, and so AI really enables us to do that. It allows us to get more accurate information. It allows us to share it more quickly. It allows us to take it and make predictions that can be helpful and that can help us to make a tactical decision that will again help us, hopefully, faithfully, and positively prosecute a war. Along those lines, there is a lot of good use that DoD has in working with its allies and trying to harness that in a way that is useful.

At its worst, however, there is a lot of risk that goes along with the automation of so many of these different systems of information. First off is the disinformation, the use of it in propaganda ways. I think we have most recently seen some disturbing aspects of it in Israel, with Hamas, basically manipulating images and manipulating data in a way that people have this propensity to believe because there is data that it is accurate, that it is actually more accurate than a human being. It is this bias. When you see something that looks like it is data and it has a picture and it comes out quickly, it is very difficult to dispel what is getting out there, and so information is being misused in certain battle spaces and can really have a perverse effect on what the local population thinks and sees and perceives, particularly when what they perceive is that one force is targeting innocent civilians or hospitals or other objects of warfare that we know we all do not want to see.

At its worst, it is dehumanizing. We hear a lot about this idea that you can have a faceless enemy, and so somebody can be killed instantly by an automatic automation algorithm versus a human who is in the loop feeling that moral aspect of the killing. That is one of the things, this ethical part of conduct, that I believe all of us in this room who care about international humanitarian law are used to feeling, which is there has to be some moral outrage or some moral value that goes along with human life in conflict.

When we get down to how the military is using this on the battlefield—and we will get into a lot more about this and how we can regulate it—there is this tremendous value of the information, the quickness, the rapidness. Even if we do not want to use it as a military advantage, we have to acknowledge that it is out there. Your enemy force is going to be using it. If we do not use it, we are disadvantaging ourselves, balanced against this risk of what can happen at its worst.

Laurie Blank

Thank you. François, let me turn to you next so that you can help us set the stage a bit more. States have been sharing their views on how international law applies in cyberspace, which has been very helpful because one of the interesting things about cyber is we do not see the state practice. You cannot actually see what a state is doing physically. What do you see as the key themes and issues in the application of international law and the evolution of thinking, both in state practice and scholarship, on cyber and international law, tying into what Sandy was saying that it is important to understand how international law is going to apply and how we are going to make sure it is incorporated? What are you seeing as key themes and issues?

Remarks by François Delerue

Thank you very much for the question, and yes, I think one of the important elements here that connects directly to what you were saying about the fact that we do not see the practice or at least we see some part of it—we have quite a limited view and sometime a bit biased as well—is the question of accountability. That is interesting because the evolution we see these days about cyber-related matters concerns predominently the question of accountability. We had this summer the recommendation from the UN Secretary-General regarding the creation of an accountability mechanism for cyber-related behavior.

What I would like to highlight here is that we saw the same trends in both the scholarship and the state positions, we had at the beginning more focus on "cyber warfare," the law of armed conflict (LOAC), *jus ad bellum*, and related questions. Then the picture has become wider with the addition of state responsibility. That has been the focus for the past ten years. The third evolution, which is what we witness today, is all the questions from specific branches of international law. Human rights, for instance, is more developed than it was before. We also see more questions about international criminal law. We even start now to see more questions related to international economic law, which for a long time was never really connected to this question of how state may use cyber operations or may use AI in cyber operations in a hostile manner.

We see also how the scholarship is influencing states and influencing their positions. But yes, what is interesting with states' positions is actually to see that it is an unprecedented practice. We have not seen in other fields states releasing entire positions, detailing their view on how international law applies to a certain types of activities. We see positions in relation to a dispute, we see it with other questions, but here this is where it is interesting: there is a double incentivization effect, it obliged states to actually think what is their position and how they interpret rules, and we see this effort going on and we see states, for example, the United States, have been publishing more than one position, and you see the evolution.

We also see how states influence each other, and I think that is an important element with the discussion we are having now, because this is exactly what we saw with international criminal law in this context. It was a topic that was included by some states, and then now it is increasingly discussed and included in state's positions.

Why this question is so important—and here, that would be my key analysis on this question—is actually again for the question of accountability. Why? Because we start to have a good picture of what is the law, what are the rules that may apply. The practice may be difficult to appreciate, but still we have kind of an idea of what is the practice, and I think states have a better idea, but they do not share it publicly.

But then the question moves to the fact that states may adopt different types of responses, different types of reactions. We have seen a lot of states adopting sanctions. The European Union has even adopted a specific mechanism for sanctions, the EU Cyber Diplomacy Toolkit. This is the big question today, and we are moving from a situation where states try to react on the state-to-state level, to a situation in which states are focusing on the individuals involved in the state practice. This is what we saw through the sanctioning. In the United States, there is also a specific practice of indictment that has been developing, and I think these observations form the rationale behind the current reflection on international criminal law.

States try to identify who are the individuals involved and to target these individuals with the objective to actually discourage states from conducting cyber operations, and I think that is an important observation for the discussion on international criminal law today, because there is this, I would say, a political dimension in the back.

Laurie Blank

Thank you. Charles, I am going to turn to you to bring the ICC into this conversation as well. The ICC prosecutor announced in September that he intends to investigate and prosecute cyber acts that fall within the jurisdiction of the ICC. Can you tell us more about the efforts to develop this policy and the questions that arise in applying the Rome Statute to malicious cyber operations?

Remarks by Charles C. Jalloh

Thank you very much, Laurie, and good morning to you all. I am going to start with a disclaimer. Unlike Laurie, I am not a rocket scientist up here. I am only a lawyer. Anyhow, would like to begin by thanking the American Society and Michael for putting together this panel and for inviting me to be part of this conversation.

I would like to now jump directly to the question that you are asking me, which was preceded by François concerning accountability, and Sandy talked about that as well. In particular, when I think about accountability, I think about the International Criminal Court, which as you all know, is a big achievement of the international community, at least in terms of the last century.

We know at a big-picture level—and this is my first and big picture point—a number of significant technological innovations that have happened in the last twenty or so years, and while those, of course, come with great benefits for states and international community, we also have to confront a number of challenges. Sandy spoke about the use of misinformation and the increasing use of dehumanization, essentially, in warfare. I think the risk that technology poses, in a sense, confront us with a trifecta: the good, the bad, and the ugly. And amongst the ugly are the malicious cyber operations that can be carried out by individuals acting privately or on the behest of states. We see hackers who are able to attack hospitals and medical facilities and other critical infrastructure, and those pose the question of where the accountability should lie, whether at the national level or the international level.

Taking the example of the United States, I believe it was back in 2012 that Defense Secretary Leon Panetta raised the specter of a cyber Pearl Harbor, a cyber Pearl Harbor warning, basically, of the potential threats that cyberattacks could do in terms of crippling the United States or its military. The same threat exists for all states in the international community.

François and Sandy alluded to the fact that a lot of what happens in this space is unknown to the public. We have a number of examples that are well known. If you think about the Stuxnet attack, which was alleged to be a joint U.S.-Israel attack on an Iranian nuclear facility back in the late 2000s, and we had the subsequent developments concerning what is called the NotPetya attack, which is an alleged attack by Russian operators against Ukraine.

The takeaway from these examples is that there is a lot happening under the shadows. The question would be, what does international law do? There is a trajectory that François tracked.

We all know, for example, the work in relation to international humanitarian law with the Tallinn Manual and so on.

That leads me then to the second point in terms of how the international criminal law regime, which as you all know, is about giving accountability to individuals for certain crimes condemned by the international community. What is critical, of course, is that in terms of the ICC statute, you have at least 124 states parties that have accepted to be part of that regime, including carrying out investigations and prosecutions of crimes at the national level. The question is when you think about the Rome Statute crimes, war crimes, crimes against humanity, genocide, and the crime of aggression, how do they anticipate cyber issues to be accommodated? Obviously, for historical reasons, we are in a position where when international criminal law was developing, definitely starting at its progeny in Nuremberg, there was no sense of what we are now dealing with in terms of some of these incredible technologies that we are seeing.

The question then becomes, in the absence of amendments to the Rome Statute by states, of course, states are slow to react in many of these scenarios, how does international criminal law come into the mix? That brings me then to the third point, which is to highlight a project that was put together some years ago by a number of governments, and I had the privilege of serving on what was called the Council of Legal Advisors on the Application of the Rome Statute to Cyber Warfare. It was convened by eleven states, led by Liechtenstein, and the Global Institute for the Prevention of the Crime of Aggression. That was in 2019 and 2020. Essentially what we tried to do in the context of that group, where I had the privilege to serve—it is about fifteen jurists from around the world—was to grapple with how the ICC could potentially fit in the existing framework, because we are not anticipating that states will be very quick to respond to the cyber challenge by creating new crimes. We all know there have been calls for that, and there is the idea of a Geneva Convention to regulate the cyberspace and so on. What do you do with the existing law? That was a question that we were grappling with in the context of that expert group.

For example, in the context of that report, we asked the question: What if a state takes control of a dam through ransomware and opens its gates, resulting in countless civilian casualties downstream? Could the nationals of that state be held accountable under the Rome Statute? If so, which crimes would that cyber operation fall under?

In another scenario, we asked separate questions concerning when you might have, for example, a terrorist organization—whether or not it is state-sponsored is irrelevant—using cyber operations to shut down the cooling system in a nuclear power plant, causing the release of radioactive materials and resulting in deaths of civilians. Those kinds of questions are, of course, obviously very important, and we see that in the context of the war in Ukraine.

I am going to make a fourth and final point, which goes directly to where Laurie was going, which is, how then does the ICC respond? The work of the Council of Legal Advisors essentially is an effort by states. It is a private, independent, expert group type of report, but it is quite significant. We also have the work of the ICRC and many others that the Office of the Prosecutor announced last August, in particular, the prosecutor Karim Khan, in a fairly provocative foreign policy piece entitled "Technology Will Not Exceed Our Humanity." Karim is more confident than I am at this point, especially when I listen to the scientists, but again, my disclaimer was I am not a scientist. He drew attention in that piece to the need for the ICC to respond. He was laying down a marker in terms of what has now become the subsequent development where in January of this year in The Hague, they convened together with Microsoft—and I thought that was very smart on his part—along with academia and civil society, and international lawyers, to have a big policy discussion on cyber, what they call "cyber-enabled crimes." The ultimate goal of this whole process, essentially, is to develop a policy paper of the kind that we have seen developed by the ICC prosecutor concerning both the investigation and the prosecution of malicious cyber acts that could potentially fall within the ICC's jurisdiction. Karim Khan has the right impulse in trying to grapple with this beast. There will be some challenges that will be interesting to talk about when we get further into the conversation. I am going to leave it at that for now. Thank you.

Laurie Blank

Thank you very much. Many issues to think about here. Let me throw out one common theme that comes up in any discussion about AI and the battle space, cyber, et cetera, is speed. The pace of everything is going to change. I am going to ask each of you, how do you see this issue, the speed of operations, the speed of decision making, the speed of reaction? How does this play out in terms of cyber operations, in terms of legal analysis, the collection of information and evidence for investigations, in terms of accountability? I will let you sort out which of those pieces you would like to address. It is a speed that we maybe cannot currently conceptualize, right? It is not just faster; it is a different magnitude. What is that going to do to all of what we are talking about already?

Sandra Hodgkinson

I will jump in first. When we get down to the accountability piece, as a DoD operator, I would not want to be at that end. The goal on the DoD side is to make sure that our people do not end up at the other end.

To speak specifically about speed, the biggest issue with the speed and the accuracy is how you keep the human in the loop. That is when you get down to accountability versus the front end. On the front end, with incredible speed, you can get great, actionable, useful, and accurate information. You can also get extremely harmful disinformation, and the speed at which that disinformation ripples through is a major problem because it also can skew the battlefield. What you need to do on an operational side is make sure that you have been able to train your people quickly enough to try to get actionable information. You have to make sure that your networks are resilient enough to filter out the disinformation that is coming through and to train those humans who are in the loop how to operate it so that you keep it protected and make sure that they are part of the decision-making chain, which will slow it down. Keeping a human involved will slow it down. You have to decide what level of human intervention you are going to have, slowing it down to try to make sure that you stay on the good side and do not end up in Charles's court. the speed is critical, but speed has to be metered by humans to try to make sure that it is accurate.

François Delerue

Speed is an important element, we always highlight that with cyber, and now it is even more important with AI. This is one of the key points. It is also interesting because now with the speed question, there is also this other question, which is what I was focusing on before, the speed at which the approach(es) adopted by states are evolving, with the fact that we still have dead angles in these approaches.

One of these dead angles that I want to highlight, building on Sandy's comments, is AI and cyber operations, which is interesting when you look at the discussion—either we have a discussion on AI or on cyber, but actually the link between the two is not that obvious at this stage of the discussion. That is something we need to think about in terms of the speed of evolution of the international discussion.

What I would also like to focus on, regarding the question of speed, is what can be referred to as a two-stage reaction system. The first stage being the reaction of the state on the spot when it faces a cyber operation and, the second stage referring to the actions states may want to reserve for a longer-term reaction after they have been able to actually dig into the operation, dig into what has been actually happening, and connecting it with other operations. One of the issues we have, both with AI and cyber operations, or when they are working together, is we have a lot of actions going on, a lot of different type of operations, a lot of different types of effects and objectives. It is thus necessary to have a long-term or broader reflection on what states want to achieve with their different reactions and in term of accountability.

One of the issues for states today, or for other actors when they think about this question, is that they have to take into account that the short-term reaction should not undermine international law. That may be one of the issues today: a state wants to react and to be able to do something, but the problem is it creates a state practice. This one is visible. It is not the same thing about the conduct of operations which is generally less visible; this reactive practice creates legal questions or legal reactions, yet this practice is so far only accompanied by general references to international law. The issue is that what states may want to achieve in the short term may actually create conditions that undermine the long-term reaction or undermine the general application and implementation of international law and questions of accountability.

Charles C. Jalloh

Thank you very much. I think I follow nicely because, at this point, we have divided the tasks. We have the operational effort on the other side and we go to François, and then you got to me because you want to avoid me. You want to avoid me precisely because of accountability, which we all agree is a fundamental premise. When you think about international law or law generally, at least effective law, you have to have compliance. The question is in the context of this discussion about amazing technologies that take humans out of the loop. The entire architecture of international law, at least in terms of international criminal law, is about individual responsibility. That was a Nuremberg idea. There was a promise of Nuremberg that there is an individual who is making a decision that ought to be told, “You know what? Some things are so beyond the pale that they constitute a matter of concern to the international community as a whole.”

For example, crimes against humanity. When you cross that line, all of us, the sovereigns, we are going to go after you. But how do you have that when you take the human out of the loop? I believe President Obama toward the end of his term put out a warning about these technologies, because when then there is no way you can attribute the responsibility to the individual, then we have a problem because we have to rethink international law.

I would say a couple of additional things that I find interesting. It has consequences both in terms of what would be the starting point if you think about the crime at issue. Let us say crimes against humanity, I am going to stay with that, which has a defined clarity at this point in Article 7 of the Rome Statute. It put the human being in terms of the individual’s conduct, but also critically, the criminal intent of the individual. How do you attribute criminal intent to a robot? How do you attribute to some kind of software platform that makes a decision that now some criteria have been fulfilled and I am going to launch that weapon? That is something that international law, at least international criminal law at this point, does not have an answer for.

The second challenge would then be how do you attribute responsibility to individuals in circumstances where one of the starting premises of the panel was precisely that there would be what they call “black-hat hackers,” so where you cannot even establish the chain of causation in the normal way that here is an individual sitting behind a computer, they press a button and we see a reaction in Afghanistan or Iraq or some other battlefield? Again, this is a huge challenge for international lawyers, not to say that international lawyers should not respond, and they are doing their best to respond. And we are doing our best to respond.

I would note as a final point that in the end, from the point of view of the ICC, regarding this operational accountability side, it is a great effort on the part of the prosecutor to say, "Look, we are going to have a conversation about this. We will have a policy paper, but because the technology is changing so rapidly, obviously we will have to keep retooling that." In a sense, that is the first effort, and I am not certain that it should end there. States, perhaps even in the ICC system, should start having a conversation within the context of the Working Group on Amendments. I do not know about politically. I am not a politician. I said I am not a rocket scientist. I am not a brain surgeon. I am going to add more things that I am not. I am just a mere lowly lawyer sitting on the corner here, but it seems to me quite wise when you have a legal regime that is a magnificent achievement of over fifty years of effort to say, "You know what? We can at least have an initial conversation within the context of the Working Group on Amendments on how we deal with this beast," because I do not think the ICC prosecutor alone would be able to target it. Thank you very much.

Laurie Blank

Okay. Everybody feeling really uplifted so far? I am going to bring us maybe down to a more tactical level, in terms of applying the law of armed conflict specifically to all of these challenging developments that we are talking about. An essential issue is the protection of civilians and minimizing harm to civilians and civilian objects. That is a core purpose of the law.

I want to throw out a couple of questions to you in this respect. We know it is axiomatic that cyber operations are becoming more integrated into military operations. They are going to occur at a faster pace. We talked about speed. Cyber is completely integrated into our everyday life. We all have a phone sitting up here. We are not even making calls, but it is next to us just in case.

We have a basic conception of what kind of civilian harm the law of armed conflict is trying to prevent. We can recite it: death, injury to civilians, damage to civilian objects. We know those. But the kind of harm that we think about from interference through cyber, through interference with satellites, all these different things that these new technologies are bringing to us, it spreads a lot wider than our traditional conception of civilian harm.

Are we going to see more widespread consequences for civilians that spread beyond these core concepts? Into the areas that we say the law of armed conflict does not address: inconvenience, disruption, et cetera. As I said, not all of those consequences fall within the LOAC concept of civilian harm. Let us think about an accountability process. It has to be responsive to victims. That is a critical piece of accountability. It is not just about the perpetrator. It is about the victims as well. How do we keep that accountability process being responsive to victims but also staying true to the law of armed conflict's core rules and principles so that we are not having accountability because I could not watch my favorite show because the satellite went down.

This harm is going to spread out geographically, way beyond the "boundaries," such that we have boundaries anymore, of the geographical space of a conflict, the parties to the conflict, when both the victims of that harm and the actors engaging in these activities are far outside the territory of the parties of the areas of hostility. You may pick at some of those questions about the consequences for civilians and how we address that, what that means for the law.

Sandra Hodgkinson

Let me kick it off at a higher level, then, because I always tend to—I was in the government when we were handling some of the early cyber war issues and trying to figure out the best way to legally handle this new threat that was coming about, and I actually found that it was very useful to fall back on the law of armed conflict. It was a very useful framework for handling cyber. At the lowest level, people were talking about cyber crime, but at the highest level with state responsibilities involved, it is a useful framework to fall into international humanitarian law.

The effort that was done to try to analogize these different cyber warfare attacks and actors into longstanding principles of distinction and proportionality and unnecessary suffering, all of which are absolutely as important as they are in cyber, are also important in this new AI world.

In a couple of areas, I am pleased that the U.S. government and many other nations are following along and looking at how IHL can inform and help govern in the AI construct, because I think the very same principles are going to matter here. The protection of civilians is going to come out of the concepts of no unnecessary suffering. And so how do you keep the human chain in there to make sure that it is not unnecessary and that it is not just statistical death, that it is not oh well 10 percent of the civilians are casualties, we will use that as an algorithm going forward and we will take 10 percent of this population out. That is the worst case of where it gets to in an automated world.

To answer your question a little bit more, though, is to take that IHL framework and just like we applied it to state sovereignty in individual actors in cyberspace, you have the same individual actor and responsibility in AI manipulation that is happening that is not all cyber-focused. It is data in many ways, not a cyberattack in all ways, but it is so analogous that I think it is very helpful that the U.S. government and other nations are taking these principles and obligations to make sure that they are training people responsibly in how to use it, that there is accountability along with the process, and that part of states will take on an obligation to make sure that their own people manage this AI in a way that follows and comports with the basic principles of international humanitarian law. You have to have that governing framework to ultimately have a framework that gets to the end where you can hold individuals accountable because there has to be something you are holding them accountable against.

François Delerue

Yes, I think these are two very important questions, how do we define consequences for the law of armed conflict and geographical or spatial dimension of the consequences and all the perpetrators for both cyber and AI operations. The first comment I would make here—and I will connect it to the previous question regarding the speed of cyber operations—is the fact that we have a longer temporality in terms of reuse of data, reuse of the operation, which may transform and expand what the consequences are.

I will also connect to what I was saying before. States may want to have a short-term reaction and a long-term reaction because they may understand at a later stage that the cyber operation observed, which may be for instance a mere violation of sovereignty with very limited consequences, may have another purpose, to reuse the data for an AI-enabled operation, to reuse for another type of operation, and thus one of the big challenges is then the fact that there is different temporality in terms of type of operations, the way they are conducted, and then in terms of their consequences and regarding the evaluation of these consequences.

In this context, we increasingly witness entangled operations involving a cyber component, as well as a physical or kinetic component, potentially also an AI reuse of the data. It is very visible in Ukraine, for example, where these different types of operations can be observed, which are connected in some way, concerning notably the identifications of targets, the collection of data, the conditioning of other types of operations. That is an important observation.

The other observation that for me is very important is that for a lot of operations, in addition to the harm identified or considered, the victim also needs to be aware and to understand this is resulting from a cyber operation. These are the consequence of a cyber operation. When your bio is taken down from the website, for instance, is it a cyber operation? Is it something else? For a lot of cases, when we are talking about these less intense cyber operations or less intense consequences, one may not think that it is the result of a cyber operation.

This is one of the big challenges today with a lot of cyber operations and AI-enabled operations—how to understand what is actually happening and how to connect and understand the consequences.

My last point was on the geographical or spatial question, and this relates to this question in the sense that yes, there are perpetrators from all over the world involved in cyber operations in armed conflict, this situation questions the geographical application of the law of armed conflict and international criminal law and other regimes, but also creates more questions in terms of gathering the information on the consequences and understanding what are the actual consequences.

You mentioned NotPetya before, and that is one of the examples where this can be observed—a cyber operation originating from the territory of Ukraine has consequences all over the globe. It was difficult to connect these different elements to understand the type of harm that was produced and how to link this type of harm to the perpetrator.

There is also an important question today on the way we approach the geographical question, the temporality question of the different legal regimes, but also how to collect the data and how to assess these different elements with regard to speed, temporality, and geographical challenges.

Charles C. Jalloh

I am always happy to go last because, listening to the colleagues, I am always provoked by, in a sense, the assumption in the beginning that there is in fact a distinction of some kind, and when you talk about harm and you measure harm definitely in the sense of international criminal law, we are talking about victims. And yet by the time we get through the conversation, we will get to François, you are talking about different treaty regimes. We started off with the principle of distinction and proportionality in the law of armed conflict and its importance, and I completely agree with that. But by the time the conversation gets to me, I think there are multiple layers of harm that could well start at the level of the individual, the victim there. What then if you have a scenario where the victim does not even want to be identified? We have had cyber attacks. There was a movie issue recently where apparently there are companies that are concerned that, if you will, the word is out there in terms of how technology has been manipulated. So even victimhood has to be rethought in terms of international criminal law to the extent that it becomes a relevant part of the accountability that we talk about.

Of course, there will be accountability at the state responsibility level, which then you are dealing with state-to-state accountability, but oftentimes that is a mask for more victims underneath.

At this stage, in terms of international criminal law, the criteria that we have will recognize at least some kind of threshold. When you talk about the law of armed conflict, you need a trigger in the first place, Article 8 of the Rome Statute. You need to have an armed conflict before you can get to that.

When you come to crimes against humanity, which are possible, there was an interesting incident that happened in Florida in a small town called Oldsmar, where someone apparently manipulated the amount of lye in the town's water supply. It is a town of about 5,000 people, and apparently, it was a very smart and astute technician who noticed that the levels of lye in the water had gone very high—to a fatal level—and then sounded the alarm and they turned that water system off. There was a big investigation. Can you imagine? You turn the water tap, and you drink and you do not know you are killing yourself. It is incredibly scary. That kind of incident, in my mind, from the point of view of international criminal law, even if we assumed the United States is a state party to the Rome Statute, would be the kind of crime under the domestic crime principle, and ought to be addressed at the level of the United States.

But there will then be the widespread use of systematic attacks of a broad scale, which is what we assume when we think about crimes against humanity, that should then attract international criminal responsibility. When you talk about victimhood in the sense of international criminal law, you would assume a certain level of threshold of seriousness and gravity and scale for it to rise to the level of the ICC prosecutor's interest. Thank you.

Laurie Blank

Okay. I am going to do one more speed round question. So many questions we could discuss, but here is one that I am still wrestling with myself, so I would like to hear what you all think. I have seen mentioned that when you mix AI and cyber, which is what we are trying to do here in this panel, we are going to start to see the autonomous development of cyber tools, cyber weapons. If I call them weapons, now I have to think about international law, and they have to be reviewed and so on, what does this mean for how we think about the implementation of the law of war? We are in an armed conflict. Let us put ourselves in an armed conflict, and because of whatever AI-enabled tools and capabilities, we have those AI-enabled capabilities are also seeking ways to exploit vulnerabilities in our adversaries' capabilities or vice versa and developing the tools to do that autonomously.

What does that mean? You are talking about a human in the loop. We are thinking about all these different things. I am going to give you guys a speed round, like a minute each to wrestle with that question. Thanks.

Sandra Hodgkinson

Okay. I will jump in quickly. I have to acknowledge the fact that those weapons are here. Trying to get states to not use them because they could be used wrongly is not going to happen, because there are going to be states that will go ahead and use them, and certainly we have to now figure out how do we use them consistent with IHL.

I still go back to the framework of before, which is we have this incredible existing body of international humanitarian law, and I think it is entirely applicable to autonomous weapons, which is that they cannot be indiscriminate, they cannot cause unnecessary suffering. When you follow all those principles, we have a legal framework that is in place. We have to start applying it, and then we have to figure out what are ways to hold states accountable that do not enforce and follow it. We should not be that scared of it, but we have to recognize that we are going to have to use that body of law.

François Delerue

Yes, I agree that they are already there, and this is already a big question. We cannot expect states to not use them or at least not be using them during conflicts, also outside of conflicts, which is an important observation, both from the geographical perspective because hostile acts tend to escape the geographical scope of the conflict in question. It is also important to recall that most cyber operations are actually taking place outside of armed conflicts, in peace situations.

There are lawyers working for the perpetrators of cyber operations. They have the capacity when they develop these technologies to actually develop them in a way that should comply with the law, and then it is more of a question, did they do the due diligence? Did they do what they had to do to comply with existing obligations, or did they just hide behind the idea that because it is a new technology, the law is difficult to comply with. There is also an important question that we will have to ask at some point in terms of accountability, not on the use, but accountability concerning the development of these technologies.

One of the big questions here, is the role of non-state actors that are contributing to the development of these technologies. This is where it becomes more complicated because a state may rely on actors that are less used to using this type of legal frameworks, and then have to take them into account for different projects, additionally most of these technologies may be the result of the combination of different technologies developed by different actors. Where does the responsibility lies to ensure that the development of a specific technological brick, which will be merged with another technological brick, still comply with the rules? There is this important challenge today in the way we develop technology or the way we aquire technology.

Charles C. Jalloh

Thank you very much, and I am glad that I am following you because, for me, my response is going to be about the last point that you made, the point about the role of non-state actors. And what I find fascinating about that is it essentially comes in two ways. One aspect of it is who has this technology, who has the capacity to develop these technologies, and we all have read that letter by Elon Musk and any number of other gurus. These are the folks who are saying please regulate. But that assumes that there is, in fact, an entity called the state that is able to regulate, and international law always assumed that because you could monopolize power in the state in the past.

There is a second concern that has been raised by cyber experts about the asymmetry. So not only do you not just have the monolith of the state that is capable of regulating, underneath that, the state itself does not have the technology to match the big tech. In fact, the technology is not in the hands of the state at the level that it is with the big tech. There you have, then, a scenario where you have purely private actors, the Microsofts of the world and so on, that are able to do a lot more than the state. Even if we put the state back in the mix, they have to turn around and rely on the technology by the private actors. I do not know what the answer to that is, but my takeaway is that it is a scary proposition for me, schooled in the territorial language of international law and that sees the state as the be all and end all. Thank you.

Laurie Blank

Thank you everyone.