Greater Good Gathering - Panel VII

Conflict

Moderator
TODD GITLIN

Panelists
ROBERT JERVIS
MATTHEW WAXMAN
LIINA ARENG
J. MICHAEL WALLER

The Greater Good Gathering held on February 6–7, 2019 explored the future of public policy and how best to advance the greater good in the 21st century in light of technological innovation, economic disruption, ideological polarization, and governance challenges. Event co-sponsors included Columbia University School of International and Public Affairs, Columbia Law School, Union Theological Seminary, The Academy of Political Science, and Public Works LLC/Brain Storm Consulting.

TODD GITLIN: I am Todd Gitlin. I teach, here at Columbia, sociology communications. I am here more as a student than as a moderator because this is not my turf, but I am eager to learn. I do want to make a couple of quick observations, joining the end of the last session.

One is that every new technology, of which I am aware, has been presented by either its inventors, or its publicists, or both as the beginning of a brand new world. A world of expanded human powers. A world of enhanced values of one sort or another. All such prognostications are half true and equally half false. What we have been through, in a kind of a whirlwind way in the last 20 years, with computer-based web projects is in the same ballpark.

It is in the same domain. The questions we ask are profound questions, but they are not profound questions because we are starting from scratch. We are always starting on a platform of existing economic structures, political structures, and cultural expectations. Nothing is new under the sun. Another thing that is not new under the sun is that new technologies are weaponized. Sometimes they begin in weaponized form.

With very early experiments in radio, for example, the United Kingdom and the United States' government were involved in making sure that radio would be used to suit their respective national security principles. That takes us to the subject of this panel, which is cybersecurity. With no further ado, I am going to very quickly name our panelists.

Liina Areng is the head of International Relations for the Estonian Information Systems Authority. She has held top positions with the Estonian Ministry of Defense as a cybersecurity advisor and with NATO. She is going to talk primarily about cybersecurity in action.

Robert Jervis is the Adlai E. Stevenson Professor of International Politics in the Department of Political Science here, past president of the American Political Science Association and the author of many books, including one with a title that seems apropos, *Perception and Misperception in International Politics*.

Matthew Waxman is the Liviu Librescu Professor of Law at Columbia. He served on the National Security Council, and then in the Department of Defense and the Department of State. In the Bush administration, he worked unsuccessfully to have U.S. captives treated in accordance with the Geneva Convention.

Michael Waller is Vice President of the Center for Security Policy in Washington, after years as the Annenberg Professor of International Communication at the Institute of World Politics. I have to add that his doctoral dissertation, which I am sure I must read now, predicted the former KGB takeover of Russia's economy and government, and has been published as a book.

Liina, you are up first.

LIINA ARENG: I am extremely thrilled to be here, following these most interesting discussions today and yesterday. It is also interesting to be a little bit of an outsider here as a European and Estonian. When I think of what I have heard today and yesterday, you have to go outside of Estonia in order to appreciate the things that are dear to you back home.

When I have heard the conversations here, I understand that many things are different here. We do not have many of the challenges and problems that you face here. The challenges back home are different. They are caused by our geographic location, our resources or, rather, the lack thereof. To start, I am trying to reflect on some of the things that struck me during the previous presentations.

I can give you a comparison of what happens in Estonia, in that respect. It was mentioned yesterday that it is very important to make the elections simpler here—easier for people to understand and participate in—to ensure political accountability. In Estonia, elections are very, very easy. For example, if we had elections today, I could just take out my laptop and my digital ID cards and vote.

All you need is internet, your laptop, and your ID card, which has a chip. It enables you to authenticate yourself and to give a digital signature to cast your vote. It was mentioned that, although surveillance and transparency, of course, are very important, it would never happen here in America. Transparency is a word that is used when you have nothing else to say.

In Estonia, transparency is essential. I think we take it for granted that we, as citizens, are the real owners of data. Transparency is very easy in Estonia. You just have to log into a citizen portal, again, using your ID card, to get a complete transaction log of all the requests of data that different public or private organizations have made against your data. You can see requests from police, hospitals, and banks. If you see any discrepancies there, you can file a request to an agency and ask for more information. If you do not see that it is justified, you can go to court. This is very, very transparent. Data and the monopoly of multinationals over your data has also been discussed a lot.

What the European Union recently adopted was a regulation concerning the free movement of non-personal data across borders. This means that it eliminates the data localization restrictions, and gives the chance for SMEs and startups to scale up and to enter new markets across European borders. That also eventually helps the creation of innovative data services and research based on big data.

Since the topic of the panel really is conflict, I have to speak also about the downsides of that digital Narnia where I come from. The downside is really the dependency that we have, in Estonia, of all the services that relate a digital way of life and that makes us vulnerable. Also, how information systems break in two ways. Either there is a technological failure or people lose trust in using them.

Trust is extremely important. In Estonia, how we generate this trust is by the Security by Design Principle. At the agency where I come from, we develop and manage the core components of our digital government infrastructure. We also operate as a cybersecurity agency. We have the system designers and system defenders under the same organizational roof. That, of course, creates a lot of friction because those who care about functionality do not really care about security and vice versa—but we think that it is a good model and we should really sustain that. To summarize, are we more secure today in Estonia than in 2007—12 years ago, where we experienced large-scale, politically-motivated cyberattacks against our public and private networks, media channels, banks, and political parties?

As a patriotic Estonian, I should probably say, yes, we are. But, since this is an academic setting and I do not know how many hackers we have in the audience who would wish harm, I am more inclined to say that I do not know. I am not sure if we are more secure today than ten or 12 years ago. Because in my own experience, over ten years now operating in this cybersecurity business and reading the news every day, we see that the attacks are getting more sophisticated.

They are getting more strategic and more geopolitical in nature. We have seen attacks against critical information infrastructure and our democratic institutions. This is really scary stuff that is happening out there. What you can do, of course, is you can filter the range of attackers by making the attack more expansive. Basically, you can eliminate the attackers that don't have as many resources. To be honest, if you are dealing with an opponent who has good motivation and large resources, which is not to say unlimited resources, they are quite probably able to get in. Then you have to deal with consequences. What can we do? We can focus on preparedness, resilience, and recovery. What is difficult for the attacker is to create persistent results.

You can take down a power grid, but depending on how much you have invested in business continuity planning, you can get it up again and continue your normal operation. It is very important to focus on preparedness and recovery. Cybersecurity is not inherently about technology but collaboration. We are investing quite a lot, in Estonia, on collaboration and community building—using people who would like to volunteer their free time to do something good for the government.

We have an organization called Cyber Defense League, which is a unit that operates under our National Guard, and is comprised of IT people from both public and private sectors who come together to exchange information and to practice or train. If there is a large-scale cyberattack happening, we can use this resource in order to fend off the attacks. This has proven an effective resource for us. On that note of collaboration and importance, that concludes my short exposé. I am happy to answer your questions.

ROBERT JERVIS: My comments will follow the previous ones very nicely. Let me just start with where you left off. This is a very complex area. A number of years ago, I was talking to one of the high U.S. government officials working on this, and he said, "This stuff makes my brain hurt." There are layers and layers of complexity here partly because the mix of technology and human factors is very intricate.

It is exactly the tradeoff between usability and security. The hack on the DNC never would have happened had the people been using appropriate prophylactic methods, but they were, as we all know, expensive and time consuming. They get in the way, and they did not use them. This complicates our lives and complicates our analysis of the situation, because it changes quite rapidly, both as the technology changes and as we adapt to it.

I come to this from having worked extensively during the Cold War on nuclear weapons and nuclear strategy. For almost all the questions, you did not have to know any physics. You just had to know these things went boom, killed many people and destroyed lots of things. You

do not have to know an atom from a schmatom. All you have to know is the basic destruction. This is not true in cyber.

A lot of the technical details matter, and they change. Let me just give one example. Matt knows this better. We used to say, maybe four years ago, that deterrence was very difficult because of the attribution problem. You could not tell who attacked you. My understanding from the experts—I have to take their word for it—is that, most certainly, the U.S. government and major players can now do attribution pretty well.

Now, they may not be able to do it immediately, and they may not be able to go public with how they know what they know, but if you read anything written, say, four years ago, they will start with the attribution problem. Nope, you have got to start with a different starting point. You get those and many other rapid changes here that make this difficult. It is often said that we are facing danger of a cyber-Pearl Harbor.

Even Leon Panetta, as Secretary of Defense, said he thinks this is greatly exaggerated. Again, let me go back to the point you made on the power grid. It is exactly what I hear from people who know much more. Taking it down is one thing. That is bad enough, but taking it down and keeping it down is much harder. The idea—that suddenly we are going to wake up and find we have been paralyzed by a cyberattack—is really very unlikely.

By the way, as an aside, Pearl Harbor, as those of you World War II buffs know, was a disaster for the Japanese because they unified the United States in a way that nothing else could have. They missed the most important two targets, the carriers that were at sea and the even more important aviation fuel that was stored near the base that would have paralyzed them. They put American battleships, which were reaching their sell-by date anyway, underwater for a year. Most of them just pumped the water out. In two years, they were sailing again. Therefore, Pearl Harbor was a disaster, but not for the U.S. The analogy just gets you thinking in the wrong way.

This does not mean that everything is fine. I would start with a point you made when you said that you do not know whether Estonia is now safer than it was 12 years. You know an enormous amount about that. I think, certainly, people I know would say the same thing about the U.S., and it is very odd. It just shows the layers of complexity here and that we are not sure how these systems respond under attack. We are not sure of the capabilities of the attackers. We are not sure of the extent to which our own systems are penetrated. We do not know how resilient to be. There is just an enormous amount of uncertainty. That is both good news and bad news. Again, that is a different world than we are used to thinking about, and it makes people very uncomfortable. There are a number of things about the cyber world that I find dangerous and potentially destabilizing.

The first is that, for most cyber tools in international conflict, it is very hard to distinguish offensive measures from what is normally seen as legitimate and often defensive, which is espionage or spying. Countries spy on each other—you find it in the Bible. You also find, if you know your Old Testament, that the spies that Moses sent came back with totally fallacious information.

There are very little changes. Cyber is now extraordinarily important in American and, I am sure, every country's intelligence. You try not only to intercept messages and decode them, but you try to get in the other side's network, get the information, and extract it the way that Russians did with the DNC and Hillary Clinton's emails. Countries are doing this on the industrial scale.

That is considered unpleasant but legitimate and, in some way, defensive because you are partly protecting yourself. The trouble is, when you penetrate the other side's nets to get information, you are also in a position to disrupt and destroy. The only difference between espionage and disruptive attack is what the payoff or the package is at the end. You, as a defender,

cannot know that until it's too late. Offense and defense are very hard to distinguish here, and that can easily lead to spirals of escalation and outcomes that no one wants.

A second troublesome aspect is that leaders are even less experienced than I am about dealing with cyber things. I could not turn on the microphone, but most of our leaders cannot even turn on their computers. I do not know what happens in Estonia, but I think, if we get a cyberattack in the United States, even if we had more qualified leaders than we do now, they would not know what was happening. The people who understand it at a technical and political level would have to convey an enormous amount of information that is difficult to get your brain around to people who probably sat through three PowerPoint presentations and had not paid attention. I would be interested to know, since Estonia has been attacked, if your leaders stay awake in the presentations and can understand them because most of the briefers are used to talking to people who understand it. When I hear them, I have to stop them every two minutes and ask questions. The gap between people who know the technology and the leadership is enormous, and that will be a problem.

In addition, if there is a crisis, the leaders will be functioning, perhaps, with degraded communication systems or communication systems they cannot quite trust. I am seeing something on my computer screen, but is it really what I am getting from the Pentagon, or is it what the Russians have hacked into? Again, we are not used to that. Another problem is that the role of third parties is much greater than in normal conflict. In the U.S., at least, and, I assume in all the Western European countries, the bulk of the targets of cyberattacks are not on the government—although they have gotten plenty. It is the banks and large companies. They are on the front lines.

The attackers, often, are little hacktivists. That is they are people who have political motives, but they are not government officials. They may just be pure criminals, or they may be criminals hired by governments. When you get an attack, in many cases, it is not attribution in the sense of where the computers that started this are, but in terms of determining who is it and what the motives are. That is difficult. Also, the companies under attack are really teched up, and there is great temptation to hack back. That is, to take offensive actions to try to disrupt or destroy the computers that are attacking them. That is illegal in the U.S. and most other countries. The banks swear, in public, that they are not doing this. Are they doing it? If they are not, my guess is they will. That is another layer of complexity.

The final one is the recent change in the American policy, ratified by Cyber Command and the Trump administration. To make a long story, it is much more assertive. It is much more trying to meet attacks forward. The Obama administration highly centralized everything, but they highly centralized decisions on use of cyber tools. The Trump administration has delegated that much further down. There are things to be said for this, but obviously, it raises the danger that people three and four levels down in the chain of command will do things without understanding the full implications—without understanding the ramifications, without understanding the political context, and without fully informing the top people. The chances for undesired escalation coming out of that are quite large.

MATTHEW WAXMAN: I want to talk about international rules for cyber conflict. Are there any? Will there be any? I teach international law. I study international law and, in particular, law and military conflict. I am especially interested in how new technologies affect law. I think about futuristic things, like cyber conflict, the deployment of AI-enabled autonomous weapon systems, and things like that, but I take a long historical view, too. I am also interested in things like sixteenth century siege warfare and the rules that governed it, if anybody ever wants to talk about that.

I find that conversations about law and cyberspace, and especially law and conflict in cyberspace, often describe the situation as a lawless kind of Wild West. The remedy for that situation that is often proposed or thrown out there is that we need a global treaty and we need rules. States ought to get together and figure out what the rules are, like a Geneva Convention for cyberspace.

I want to say that I think that initial description of the Wild West is not accurate, though. Nor is the proposed remedy of a global treaty realistic, at least not for the foreseeable future. First, let me talk about why there is no global cyber treaty. We have many treaties governing conflict, like land warfare, for example. We have global treaties for maritime law. First of all, it is important to keep in mind that those laws developed over the course of centuries. It was finally in the twentieth century that they were codified. We are talking about, often, very long processes for the development of international law. I think there are three specific reasons why developing a treaty to govern conduct, especially conduct in conflict in cyberspace, will be very difficult.

One is because the interests of states are just not aligned on these issues. There are certain questions on which states can agree. But there are a lot of issues on which states do not agree because they have different levels of power, different methods of conflict, different capabilities, and different ways in which they use cyber technologies, domestically, as part of their own domestic governance or with regard to their own domestic polity. Not only are states' interests not aligned, but states do not even quite know what their interests are in this area. I think, if you were to ask U.S. government officials what they would want in a cybersecurity treaty, it would be very difficult to pin the U.S. government down. You would get different answers in different agencies.

Putting it most simply, parts of the government want very permissive rules because they want to go out and be able to do a lot of stuff against other states or non-state actors in cyberspace. Other parts of the government are very interested in defense and maybe interested in very restrictive rules. Therefore, interests are not well aligned.

A second factor making the development of international law difficult, especially in negotiation of a treaty in this area, is the low visibility of actions and reactions in cyberspace. Bob talked about some of these. Even if activities are detectable by the intelligence communities' intelligence agencies, they are often not very publicly visible. Monitoring and enforcing compliance with treaties is likely to be extremely difficult in this area.

Finally, I have a point I alluded to earlier. Bob mentioned complexity of cyber issues. It is complexity, combined with speed. It is the development of newer and newer technologies and, therefore, newer and newer methods of conflict. One thing about international law or law generally, is it tends to move slowly. Technology, on the other hand, tends to move quickly, and the pace of that change is ever accelerating.

There is a general challenge in the area of cyber law, both internationally and domestically. Can law keep up with changes in technology? Those are reasons to be pessimistic about the prospects of a global treaty. Let me give some reasons for some optimism, in that, there are and will be greater development and clarification of international rules and international norms in this area.

One is that there are a lot of global conversations going on. A lot of them are not reaching consensus. However, there is a lot of diplomatic effort among states devoted to trying to negotiate, clarify, and develop rules in this area. Increasingly, civil society in the private sector is inserting itself into those negotiations and development and, perhaps, in some productive ways.

I think one interesting phenomenon in this area is that, because so much of the global digital infrastructure is controlled by private hands rather than states—which holds a monopoly on a lot of the instruments of kinetic violence—private industry may play a much greater role in

setting some global rules for conflict in cyberspace than it does for other areas of conflict. At least, I want to pose that as a question to think about and consider.

There is a lot of action among states trying to interpret existing international law, existing laws of war, existing application of the U.N. Charter, rules of self-defense, and rules about state sovereignty. How do long-standing rules apply to new technologies? Some of the applications and contexts are new, but many of the legal concepts are long-standing.

Overall, I would say I am more optimistic about the development of international law in this area and international norms for cyber conflict than those who say that there are no rules yet and that it is a Wild West situation. I think there is a lot more going on and a lot more content to global governance of cyber conflict, but I do not expect the outcome of these negotiations to look like rules for other forms of conflict. I do not expect it to look like a Geneva Convention for cyber conflict or a U.N. convention on the use of cyber weapons, as a model for what international rulemaking will look like.

J. MICHAEL WALLER: The Internet was created as a weapon and only later adapted for civilian purposes. There is a historic marker in Arlington, Virginia—one of the "George Washington slept here" type of cast iron markers—marking the invention of what became the Internet, by a Pentagon agency. When we think about it as a civilian product, first, we really have to think that it was designed as a weapon.

The core root servers of the Internet, to this day, run through the Pentagon. The problem is, how do we as civilians manage that when you have civilian companies and non-state actors using those same systems and same root servers? Whether it is Facebook, Twitter, or a terrorist organization—all using the Pentagon's root servers to communicate and to commit whatever acts, good or bad, that they might do. How do we manage that?

Then, as a society, how do we manage defending that and waging conflict through that? Added to that, the traditional military chains of command are, by nature, very slow and deliberative. The political chains of command over the military are generally very slow. The diplomatic system is usually very slow and deliberative. Then things need legal review, which is often extremely slow. Even running covert operations through the intelligence services, by nature, is very slow because each covert action needs the President to physically sign off on what is called a finding. You have these very slow and cumbersome pre-digital decision and command systems—then the rapidity of how cyberspace really works, then how non-state actors work, and then how any of us, potentially, can start or participate in a world conflict, if we choose to.

It is a really powerful thing when you think about it. Then you think of the legality, the morality, and the ethics of that. Like it or not, whichever side you might come down on, the Arab Spring was definitely a cyber-driven conflict. The Iranian Green Revolution attempt, in 2009 previously, was very much a cyber-driven conflict—driven around the world by Iranian ex-pats and their supporters to support the people inside Iran against the regime.

Subsequent attempts were as well. The current situation in Venezuela is largely a cyber-driven conflict. You have a hybridized version of private initiatives on the Venezuelan side. Private initiatives of the single United States Senator who happens to speak fluent Spanish and chairs the Western Hemisphere subcommittee (whose state, Florida, has a lot of interest in all things Latin America). Then certain people in the State Department and throughout the government all supporting a very broad-based coalition of Venezuelans. Getting a lot of bipartisan support and then getting some of the broadest possible international support in a very rapid fashion that did not take place through our traditional embassies using those systems.

It took place mainly through Twitter. If you look at how these various governments around the world started recognizing Juan Guaidó as the interim government of Venezuela—that was mainly done through Twitter. You are finding now that the whole diplomatic process,

in that case, was sidestepped. The Western Hemisphere Affairs Bureau of the State Department was sidestepped in favor of a former government official, Elliott Abrams, who was brought in to supervise this through the National Security Council, bypassing the whole State Department bureaucracy.

What does that say about embassies and how they work? What does it say about state actors, in general, if this is an internationalist movement that is supporting a government because, according to its constitution, the parliamentary speaker can proclaim himself to be president in the event the actual president is abusing office. It is a very unusual situation. Then you had this crescendo of diplomatic recognition from Donald Trump to Justin Trudeau, polar opposites politically, and then a big follow-on after that.

It was a very remarkable thing. If you follow it every day, it can be very exciting. If you think about it more, it can also be very disturbing. One of the disturbing elements of this, which has been brought up a lot during this event, is how this battle of cyberspace was used to interfere in our elections. It is a big problem. Even if not all the facts are in, and even if some of the facts are not yet examined to their fullest, you have Russian attempts, successful or otherwise, to interfere in our elections.

We get very alarmed at this in the 2016 election, but then you put it into perspective that Moscow has interfered in our elections ever since about 1920, when Moscow controlled the communist party in the United States, running candidates. They were funded and directed by Moscow, under discipline to support whatever Soviet line was pushed at that same time. It only broke up around 1988 or 1992, whenever the party stopped running its candidates.

So, we have had this over a long time. They are just doing it a different way now. Putin has a different way of doing it. We should step back, not become so alarmed at it and recognize that is their traditional way of state craft over the past century. How can we combat that? We sort of gnash our teeth and wring our hands, knowing this is happening to us—asking what are we going to do?

First, you have your investigative capabilities that are very well underway. You have, specifically in Europe, counter disinformation—privately and publicly funded entities that are doing a great job in different perspectives on countering Russian disinformation and propaganda. But we have not done anything yet to build a retaliatory capability or a deterrence capability. This is something that is relatively easy. It is cheap. It is humane. It is nonmilitary, but it can really cause a lot of headaches for those dictators, like Putin, who want to interfere in our democracies and undermine us. Who has trolled Vladimir Putin? He reads his German and Russian language Twitter accounts. He tweets on his own. If you follow him, his real tweets have his initials on them. He has a thin skin and a huge ego. People who knew him when he was a teenager said he was a very different type of predator, but he was always a bad person. There is so much dirt on him. Imagine a Wikileaks set up to mine the private information of his inner circle and to make it public, on a private-sector basis, or having intelligence services do it and spill it out.

There are many things that can be done. We are only digging up dirt on certain oligarchs who he really depends on. He cannot rule without the support of those oligarchs. It is not easy to know who they are. This information is already collected mainly by people in London. It is available in Russian and in English. It is not difficult to do. There was a case where Ukrainian hackers got into the email accounts of one of Putin's right-hand people and published those online. It was terribly embarrassing. This was right at the time that the Russians invaded Ukraine. The same group of hackers took down the power grid in Crimea. Then, when it did not stay down long enough, they went and blew it up. They hacked into the Russian command and control and issued false orders for the invading forces to confuse the troops, confuse the tank movements, and everything else.

This was just a group of less than ten people with no budget and without the authority of their own government, because their own government was too corrupt to really defend their country against the invaders. This is a case of citizens' self-defense of their own country. They were doing it in connection with the militia groups that they had set up to defend Ukraine against the invaders. This whole area of cyberspace in conflict is flipping the way we do traditional statecraft on its head.

It takes longer to write an academic paper on certain things than it does to change the ways of doing things. Therefore, the opportunity is here for anyone who wants to engage in conflict, defend against conflict, deter against conflict, or retaliate against conflict, without escalating up the military scale. It is also going to change the way we do intelligence covert operations. It is also going to change the way we do diplomacy, when we find the increasing obsolescence of traditional embassies in traditional diplomatic processes. Thus, this is a huge battle space that we have just begun to explore.

GITLIN: Thank you very much. We are almost out of time. If anyone on the panel would like to respond, you have that opportunity. We can handle one simple question.

QUESTION 1: Thank you so much for giving me an opportunity. I am a reporter on fintech, block chain, and crypto. Every time I read something about the Estonian government using block chain technology to build up their cybersecurity system, I am always very excited. My question is, what do you think the block chain can be further used and developed for in the Estonian government? What could be the useful lessons offered to NATO allies to better use this technology? Thank you.

ARENG: Block chain is, I think, the future technology that will increasingly be used to protect the critical infrastructure and different information systems. We have used block chain since 2012. We started testing it in 2008. I guess we are one of the first use cases where we use that in government as distributed ledger. It is obviously an effective method. We have exported that also to the states.

The Department of Defense and Lockheed Martin are using that. So, it is spreading. That is, I guess, a quality stamp. It is technology to stay. I do not know whether that will survive the quantum surprise that we are all waiting to see. How and when do we have to move our critical assets to another technology that would survive the quantum technology? Block chain could be one of the solutions so far.

ABOUT THE PANELISTS

TODD GITLIN has written 16 books including history from the last century, *The Sixties: Years of Hope, Days of Rage* and contemporary, *Occupy Nation: The Roots, The Spirit, And The Promise of Occupy Wall Street*; sociology, *The Whole World is Watching: Mass Media in the Making and Unmaking of the New Left*; communications theory *Media Unlimited*; and three published novels, including *Sacrifice*, which won the Harold Ribalow Award for fiction on Jewish themes. He is a frequent contributor to the *New York Times*, *Washington Post*, and many magazines.

LIINA ARENG assumed the duties of Partner Leader of the European Union Cyber Resilience 4 Development Project in 2018. She provides strategic guidance and advice, coordinates and implements Estonian contribution to this project focusing on cyber capacity building in Africa

and Asia. From 2014 to 2017, Ms. Areng served as Director of International Relations at Estonian Information System Authority, a central governmental agency responsible for cyber security and e-Government information systems. Prior to that, she worked at the NATO Cooperative Cyber Defence Centre of Excellence as Head of International Affairs and was awarded an honorary title of NATO CCD COE Ambassador. Between 1999 and 2012, Ms. Areng held different positions in Estonian Ministry of Defence, including Cybersecurity Adviser and Counsellor at the Permanent Representation of Estonia to NATO in Brussels. She has also worked as a research fellow in NATO Defence College in Rome.

ROBERT JERVIS is Adlai E. Stevenson Professor of International Politics at Columbia University. His most recent book is *How Statesmen Think*, and his other books include *Why Intelligence Fails: Lessons From The Iranian Revolution and the Iraq War, American Foreign Policy in a New Era*, *System Effects: Complexity in Political Life*, and *The Meaning of the Nuclear Revolution*. He was President of the American Political Science Association in 2000-01, has received career achievement awards from the International Society of Political Psychology and ISA's Security Studies Section, and was awarded honorary degrees by the University of Venice and Oberlin College. In 2006, he received the National Academy of Science's tri-annual award for behavioral sciences contributions to avoiding nuclear war.

J. MICHAEL WALLER is Vice President of the Center for Security Policy in Washington, where he focuses on unconventional forms of conflict and conflict resolution. For 13 years, he was the Annenberg Professor of International Communication at the Institute of World Politics, a graduate school of national security affairs in Washington, D.C. He has been a lecturer with the Naval Postgraduate School and the John F. Kennedy Special Warfare Center and School. Dr. Waller is a founding editorial board member of two peer-reviewed journals: *NATO's Defence Strategic Communications* journal and *Demokratizatsiya: The Journal of Post-Soviet Democratization*. He earned his Ph.D. in international security affairs from Boston University in 1993. His doctoral dissertation predicted the former KGB takeover of Russia's economy and government.

MATTHEW C. WAXMAN is the Liviu Librescu Professor of Law and the faculty chair of the National Security Law Program. Waxman is an expert in national security law and international law, including issues related to executive power; international human rights and constitutional rights; military force and armed conflict; and terrorism. He clerked for Supreme Court Justice David H. Souter and Judge Joel M. Flaum of the 7th U.S. Circuit Court of Appeals. Before joining the Law School faculty, he served in senior positions at the State Department, the Department of Defense, and the National Security Council. Waxman was a Fulbright Scholar to the United Kingdom, where he studied international relations and military history. He is a member of the Council on Foreign Relations, where he also serves as Adjunct Senior Fellow for Law and Foreign Policy, and he is the co-chair of the Cybersecurity Center at the Columbia Data Science Institute.