Turtle Bay Security Roundtable

Managing the Next Generation of Weapons Threats

Wednesday, March 26, 2014, Japan Society

On Wednesday, March 26, 2014, the Permanent Missions of Japan, Turkey, and Poland to the United Nations hosted the Turtle Bay Security Roundtable: Managing the Next Generation of Weapons Threats. The seminar was held in cooperation with Stimson, a civil society think tank focused on global security. The three-year-old forum offers a crucial opportunity to engage in frank, candid discussions while getting the chance to collect outside views and opinions from learned experts. The sixth meeting of the Turtle Bay Security Roundtable examined the diffusion and potential use of new, technologically-advanced weapons, while also considering innovative approaches to their control by applying the lessons of previous nonproliferation and arms control efforts. While States focus on obligations related to conventional weapons, other weapons systems – mostly outside the scope of the Arms Trade Treaty (ATT) and other conventional control mechanisms – have emerged as potential new challenges. About 90 participants representing around 40 UN Missions as well as prominent nonproliferation experts and members of civil society engaged in an interactive and in-depth discussion on this complicated yet timely subject.

Opening Remarks

Ambassador Motohide Yoshikawa of Japan opened the roundtable by emphasizing its relevance given recent current events, from North Korea's missile launches to the General Assembly resolution vote on Ukraine. Ambassador Yoshikawa also remarked on the large attendance of that day's roundtable and said that the wide, devoted audience proves the need for these meetings.

Referring to the specific topic chosen for the March 26th meeting, he claimed that it was clear to him that there are distinct benefits to technological advancements. However, absent requisite controls, these new types of weaponry also have the potential to complicate the international security environment.

Ambassador Halit Çevik of Turkey explained that military technology is advancing at an unprecedented pace, new categories of weapons such as cyber-weapons are emerging, and battles without the presence of humans on the field are no longer part of science fiction. Sharing his views on autonomous weapons systems and unmanned aerial vehicles (UAVs) and stating that information technologies have become an enormous strength, but also the "Achilles heel" of our modern civilization, he drew attention to the challenge of cyber-terrorism and to the increasing lethal capacity of modern weapons. Therefore, he stressed the need to establish proper norms, regulations and control systems.

Ambassador Ryszard Sarkowicz of Poland began by explaining that we are at the beginning of a very complex discussion and we should aim to explore and discuss the many differing perspectives. Ambassador Sarkowicz also said he is convinced that the Turtle Bay discussion would have a positive impact on our common understanding of both the threats and potential responses to these emerging technologies.

First Session: Next Generation of Conventional Weapons

Panelists: Brendan Conlon, Vahna, Inc., Cyber Security Solutions; Ben FitzGerald, Center for a New American Security; Micah Zenko, Council on Foreign Relations. Moderator: Brian Finlay, Stimson.

Brian Finlay started the session by stating that much work has been dedicated to managing threats of the 20th century, but that future generations of technology require diligence now in order to anticipate threats that currently reside over the horizon. The lessons accrued in the past on how to manage technological advances need to be applied to the future.

Finlay first engaged Ben FitzGerald. When asked about the two or three technology spaces that keep him awake at night, FitzGerald responded that he is concerned about the convergence of a number of trends and the inherently unpredictable results from that confluence of technological advancements. When technology diffuses outside of governments, it would be hard to tell how important one individual trend may or may not be. In addition, there should be concern with major powers because we have not yet created norms and do not know how one should act with the power of technology.

In Libya and Syria, for example, non-state actors were able to develop armored vehicles and link iPads to bombs, perpetuating a long conflict with a much larger and more powerful actor. While guerrilla warfare is not new, although this level of sophistication is. FitzGerald also discussed the uncertainties there are with experimenting with synthetic biology and human performance.

Turning to UAVs, Finlay asked Micah Zenko to paint a picture of their current technological state and use. Zenko said that UAVs—known colloquially as drones—have emerged in a handful of countries. They have taken off quickly in Israel, the US, and the UK, among others. States have used drones for things they would never have considered in the realm of traditional warfare, such as shooting drones out of the sky, demonstrating that methods of war have changed. Although not a pervasive threat, in the future, their presence and use will be inevitable. Replacing humans is the ultimate goal, since humans are expensive. Hezbollah has drones, but Israel is rightly more concerned about their rockets and the damage those can inflict. Zenko said that if he were a non-state actor, he would be thinking about the many other ways to inflict harm that are less expensive than drones. As for the future, Zenko said that eventually UAVs will be deployed everywhere and move beyond military uses. A whole different conversation can be had about cyberspace, which requires a different conceptualization and is very intangible with its own sets of unique challenges.

Brendan Conlon started by explaining that cyber can mean anything someone wants it to mean, and that one aspect of it is how rapidly new technology can be turned around. Once a tool is developed—for example, the Stuxnet virus—it can easily be used by other actors, including initial targets of the tool. The transfer is almost immediate. As for where the technology is being innovated, it is everywhere: from government organizations to civilian companies. However, their focuses differ. Conlon believes industry is the leader when it comes to the defensive side of cyberspace technology. Meanwhile, the government has invested more heavily on the offensive side. When asked to discuss the future of non-state actors in cyberspace, Conlon responded that we must move past the lone hacker myth.

The floor was then opened for an interactive portion of the discussion, during which many participants asked for more information about drones' possibilities. When asked how international legal regimes should respond to this eventuality, the panelists agreed that since technology moves so quickly, a forum is needed to determine norms and establish policy in a timely manner. Panelists replied to a question posed about the quick pace and whether advanced states will always have the advantage and the simple answer was "no" since, as things advance, everyone will exploit their own niche and cited the Syrian Electronic Army as an example.

One of the last questions asked concerned what one thing the UN should be doing to manage the challenge and what the audience should make sure to cable back to their capitols. All panelists responded and Zenko stated that clarification from the states with UAVs must be demanded. When the closest allies to these countries care about what they are doing, the countries will do their best not to make waves. The problems should be made apparent. FitzGerald replied by mentioning the UN and its members and how each need to develop and advocate more sophisticated mechanisms with which to deal with emerging technologies. The technology discussion should be mainstreamed and a happy middle could and should be found between policy strategy and technology-speak. Crucial distinctions must be made between what is a technology problem and what is a legal problem. Another area for the UN to work on is speed of response. Zenko said the model for the UN is its space policy. The UN has many different areas and groups at its disposal. No other body has the convening power and moral authority.

Second Session: The Evolving Toolkit for Prevention

Panelists: Hugh Griffiths, SIPRI; Matthew Rhoades, Truman National Security Project; Mary Wareham, Human Rights Watch. Moderator: Rachel Stohl, Stimson

In the second session, Rachel Stohl, took a look at existing control regimes, like the ATT, NPT, and sanctions, as well as new regimes, that the United Nations could use to tackle the challenges of new weapons technology. Stohl wondered how we can be proactive, not reactive, to these challenges with out of the box approaches.

She began with Hugh Griffiths, an expert on sanctions. In a detailed discussion, Griffiths explained how a recent SIPRI study found that a majority of companies and individuals going against the sanctions ban are not registered with North Korea and shipping companies become unknowing victims for smuggling. The global supply chain offers many opportunities to those keen to evade bans because it is very fast and it is extremely difficult to trace items due to the anonymity of shipping containers. The transportation and logistics industry must be more involved with this process as to gather and provide more information about the nature of shipments. Increased involvement essentially calls for a layered approach. By getting "buy-in" from various stakeholders, it would allow sanctions regimes to receive shipping routes and all governments to access shipping systems. However, this is difficult in the current climate. For example, in Dubai, a UAE customs official may inspect some goods and not realize they are dual-use items that fall under prohibition because the export license does not accompany the goods.

Stohl switched the conversation from how to improve current rules to creating ones for systems that do not exist yet. She asked Mary Wareham how we should address fully autonomous weapons and what has been done on this front already. Wareham gave a summary of what has happened since the Campaign to Stop Killer Robots began 18 months ago. Many meetings involving concerned parties, from roboticists to governments, have happened and will continue to take place this year. There is a large risk of an arms race here, Wareham contended. Wareham said that HRW is urging work on this issue on any level. A precedent to follow in this case may be how lasers were banned in the 1990s. Laser weapons did not exist but the international community recognized their potential challenges and worked ahead. HRW is looking for some sort of product by November 2016.

Cyber, once again, is a whole different issue to tackle. Matthew Rhoades of the Truman National Security Project said that attribution in the cyber sphere is very difficult because there are a number of sanctuaries for non-state actors. Turning to stateon-state action, there are two scenarios. First, cyber tools may be involved in kinetic warfare. This is very possible, as already it is being used more and more in traditional warfare. The second scenario of state-on-state action would be hostilities just in the cyber realm, but Rhoades says there is no incentive to attack but not take credit for the action, which makes this a questionable tactic. In this latter case, states may just use a proxy, which was seen in Estonia in 2007 and Georgia in 2008.

Given all the unknowns in the cyber sphere, Stohl asked Rhoades what states, the UN, and/or multilateral regimes can do to protect their interests. In response, he said states must figure out their threshold for infractions. Until the threshold is met and communicated to the world, the advantage will be with the aggressors since there are no boundaries. The near term goal in this area is the definition of vocabulary: what constitutes an armed attack, how should the terms of distinction and proportion be applied in the cyber area, etc. By focusing on low hanging fruit that many agree on, like cyber-crime, there will be an opportunity for states to get together to share responsibilities and information. All agreed on information sharing and governments using existing regimes while still innovating.

The interactive portion of the discussion contained many questions about how to better improve sanctions regimes. Griffiths said that everyone is concerned about mass data gathering along the lines of what he suggests would be helpful, especially since the Snowden revelations. However, the mass gathering of this data could be used as an excuse by countries not to ask. Meanwhile, it must be recognized that trying to stop land smuggling is a whole different issue and much harder.

When asked to grade the progress in finding solutions to these problems so far, most of the panelists were positive. Wareham would give the UN an A at the moment due to its high level of engagement. The challenge for governments is getting to the necessary detail and expertise on these issues. The U.S. is able to be fully involved in the conversation, but she worries about other countries. Meanwhile, Rhoades said states are very uneven and within states there are differences between offensive and defensive capabilities. Ms. Stohl concluded by saying that the tools are in place and that what is needed now is a common language and the initiative to take advantage of what the private sector has to offer. Ask questions and use the data.

Keynote Address

Duane Andrews, Former CEO of QinetiQ North America

Duane Andrews started by giving a little background of his experience in this field. After spending eleven years in the Air Force, he joined the newly formed House Intelligence Committee. In 1989, Andrews became the Chief Information Officer of the Pentagon, tackling such issues as information security and the threat of information warfare. When he joined the private sector he dealt with a range of topics, from robots to container security.

He agreed with the panelists that technology is evolving much faster than the methods of control and regulation and that definitions are still needed. Andrews stressed that any controls we create, though, must be marked by flexibility. If they are not flexible, the controls will be obsolete by the time they are implemented due to fast-moving technological innovations.

All the innovations have some common threads that must be considered. Andrews listed them succinctly: the technologies are ubiquitous, the potential perpetrators are globally dispersed, the technical understanding to operate the technology is readily available, the technology is not subject to effective control regimes, and they compose mostly dual-use items embedded in civilian areas. Andrews spoke of three important areas of concern: cyber, unmanned weapons, and nefarious information proliferation.

The first warning about the dangers in the cyber realm came three decades ago. Despite studies and attacks since then, there has not been much progress in understanding how to secure this field, much less toward finding a solution. While difficulties remain, discussions on this topic must continue.

The second area of concern lies with unmanned technologies. The threat differs here because it involves specialized hardware and software that doesn't readily fall under controls. Components of weapons can easily fall into the private market, legally available. For example, you can buy parts of planes and create your own improvised drone quite legally and easily. Therefore, this becomes a whole different challenge. Should we shut down the toy industry because they use parts that could be turned into weapons? We have to consider how to regulate items that may become commercial.

Finally, Andrews spoke of "nefarious information proliferation," when old technology can be adapted for new, harmful purposes. For example, the internet has created a pathway for anyone to get instructions for anything from bombs to poison. These are threats to civil order and while Andrews was clear about not advocating censorship, he also said that the consequences must at least be considered.

In the end, he concluded with what delegations to the United Nations can do, such as find ways to raise the awareness of dangers to public society as a way to gain support for regulation. Andrews did not want to minimize the challenges that lay ahead: this endeavor means dealing with bureaucracies, private industry, and the public, but having discussions should help and make us ready for the future.

Andrews was asked several questions in response to his keynote speech. For the first question about the challenges of enhanced public-private partnerships, he replied by instilling confidence that there are enough strategic thinkers and patriots in industry to hold a dialogue together. He also said that industry is suffering as much from cyber as governments are with time and money, therefore there is incentive to work together. He was then asked how to improve this important collaboration, and Andrews replied that governments must take the next step and initiate such programs. Roundtables and discussions like the Turtle Bay Security Roundtable are great to get participants in all areas talking and get beyond brainstorming.

Concluding Remarks

To conclude the day, Mr. Łukasz Zieliński, Deputy Permanent Representative of Poland, reiterated that these topics are indeed a novelty and discussions like the one at the roundtable play an important role in facilitating new ideas. Counsellor İlker Kılıç of Turkey said that some fears that were raised in the discussion, that this was only natural, as "change instigates fears" and more so when it breeds potential for increased lethality. Since technological advancement is a double-edged sword, we must work together and with industry to prevent calamitous events. Ambassador Motohide Yoshikawa of Japan continued by stating that advancements are happening so fast that, while we enjoy their benefits, we must also understand how to reduce negative consequences. He said that we can make use of tools already available, though the blurred line between military and civilian use poses challenges. He ended the day in hopes that the discussion gave everyone some new ideas with which to work.