An Interview with Congressman James R. Langevin

How have the threats facing the United States evolved in the 16 years you have been in Congress?

When I first came into Congress, we were still in that transition phase of going from a relatively calm and stable, bipolar world with the United States and the Soviet Union as chief adversaries. We were just entering the multi-polar world in which we live and the world became much more paradoxically unstable and the threats became more involved and grew. I came in around 2000—before 9/11—and none of us could have anticipated how the world would change so dramatically, on that date in particular, and later morph into other threats and challenges.

Now we have threats of international terrorism. A resurgent Russia is a challenge to the United States and to the international community. There is the growing challenge of China and their cyber activities, as well as the challenges China poses to U.S. interests in the Asia Pacific region. And you have the nations of Iran and North Korea—particularly the nuclear threat coming from North Korea. And then of course, one of my primary focuses is the challenge of cybersecurity. I often say that cybersecurity is the national and economic security issue of the 21st century. All those things have emerged and morphed since I first came to Congress and I do not see this challenge as diminishing any time soon.

The U.S. House of Representatives Armed Services Committee (HASC) Subcommittee on Emerging Threats and Capabilities (ETC)—please explain its mandate and priorities.

Much of the work in the ETC focuses on trying to confront our immediate challenges but also staying one step ahead of our adversaries, and the challenges that we face on a number of levels. Our subcommittee

This interview was conducted by Ms. Patricia Clough in October 2017 and updated early this year.

has jurisdiction over U.S. Special Operations Command (USSOCOM); U.S. Cyber Command (USCYBERCOM) and some aspect over the National Security Agency (NSA); and all Department of Defense (DOD) research and development programs. This includes the Defense Advanced Research Projects Agency (DARPA) and the work of the Office of Naval Research, as well as counterterrorism, counterproliferation, and information warfare-type programs. All of those elements confront not just immediate threats but also look down the road as to how we meet the emerging threats and challenges to our security. The ETC is perhaps the most interesting and challenging of the subcommittees, which is why I have stayed on it from the very beginning.

When I first got on the HASC it was the Research and Development (R&D) Subcommittee and I also was on the [separate] terrorism panel. We were limited by [House] rules on the number of subcommittees that we could have, so the HASC could not add another subcommittee. So what had existed prior to my arrival and had continued on for the first term of my time was the terrorism panel, which was relatively new and did not have the same power as a subcommittee. After 9/11 the HASC combined the R&D subcommittee and the terrorism panel to become-the Emerging Threats and Capabilities Subcommittee.

You mentioned USSOCOM—our Special Operations Forces primarily have been focused on counterterrorism but they recently assumed responsibility for countering non-strategic weapons of mass destruction. What new capabilities do our Special Operations Forces need, if any?

USSOCOM is still adapting to those additional responsibilities, but they are well-resourced in terms of people, training, and capabilities for their [new] counterproliferation mission. I am confident they will continue to do the job we expect.

What are your major concerns regarding the proliferation of WMD and the potential intersection with cyber and terrorist attacks?

There is a range of concern. Certainly nuclear proliferation is a chief challenge that we face, with North Korea as our primary adversary—the enemy that we need to be more concerned about and confront. Because as more fissile material is created you run the risk of that material getting into the wrong hands. The difficult part in creating a nuclear weapon is not developing the design—unfortunately, that information is readily available on the internet. The difficult part is getting your hands on fissile material. So anytime there is more fissile material out there in the world, you run the risk of it getting into the wrong hands.

This is something that has always worried me—if a nation-state sells fissile material to an individual or terrorist group, they may use it to make a nuclear device or to make a dirty bomb using radiological material. This worries me the most. Some radiological material is commonly available. Cesium, for example, is found in medical testing equipment and is the consistency of salt. If [a small amount of] cesium was dispersed through a traditional explosive device it could deny access to a significant amount of area for an extended period of time. Not only is there a physical threat, there is also psychological concern. North Korea is an enemy of the United States—what they might do with their fissile material concerns me.

As for the other emerging threats—chemical and biological threats worry me, as do cyber threats. What years ago could only have been achieved through use of kinetic weapons can now be achieved through a use of a few key strokes. A cyberattack on our electric grid could wipe out large portions of the grid for not just days or weeks, but potentially months.

When I first came into the [emerging threat] field, I chaired the subcommittee within the House

Committee on Homeland Security that has jurisdiction over cyber issues. My work there carries over to the ETC subcommittee. Sophisticated cyber actors, such as China, Russia, North Korea, and Iran threaten the United States as do individuals, terrorist organizations, and criminal enterprises. Nation-states give proxies the tools to carry out cyber operations to avoid having the nation-state's fingerprints on the operations. This keeps me up at night. Nation-states might have the worst weapons, but they lack the will to use them. How long will it be before the worst weapons get into the hands of someone or some entity that has the will to use them?

State and non-state adversaries have successfully adapted to the cyber age; what can the United States and our partners do to sustain our technological superiority?

Here is where we really need a whole-of-government approach. The [U.S. Department of State (DOS)] Global Engagement Center (GEC) was created by the previous Administration to coordinate counterterrorism messaging [to foreign audiences]. I have been very disappointed in the current Administration's limited use of the Center, for which the Department of Defense (DOD) plays a supporting role. The lack of stability and consistency in senior leadership positions within the DOS—and particularly in their oversight of the GEC—does nothing to instill confidence in this very important effort. It is imperative the United States uses the Center's robust capabilities and responsibilities to counter the messaging from our enemies—both terrorist organizations such as Islamic State of Iraq and the Levant or al-Qaeda in their recruitment efforts, and nation-states who use disinformation to sow discord in an attempt to weaken democratic institutions in western societies. It is noteworthy that the DOS has finally accepted $40 million in transfer funds from the DOD to assist in this effort. But we cannot, and should not, do this alone. We need to work with our international partners on counter-messaging. Terrorism and brazen threats to democracy are not just problems for the United States, they are international problems, and we need to be working on this together.

What would that collaboration look like?

We must ensure that we are using all of our capabilities to identify terrorist organizations that are trying to use their messaging capabilities to recruit and operationalize, whether it is domestically or overseas. The Federal Bureau of Investigations and Department of Homeland Security have the internal mission, which is not our role here in the ETC Subcommittee. But certainly overseas is something the ETC ought to be focusing on—is the United States using its capabilities in a robust way, making sure that we are working with our international partners to fight or countermessage?

What our Special Operations Forces might need for the fight—should the United States focus on acquisitions (software or equipment), technological know-how, or training?

USSOCOM already has vast acquisitions authority and rapid prototyping. Although, rapid prototyping is something we really ought to continue to support so that we get the best technologies in the hands of the warfighters. We have done some good work on that—separating out the research and development work from the acquisitions piece so that things function more appropriately. Still, there is more room for progress.

Rapid acquisitions versus over-the-horizon capabilities—how should the United States prioritize these needs?

That is where research and development comes into play in our subcommittee. How do we overcome the "valley of death?" Getting the technologies out of the lab and into the hands of the warfighter is always a challenge. As is overcoming cultural barriers. The

Pentagon loves their legacy capabilities and technology. We [the ETC, HASC, and Congress] sometimes need to prod the Pentagon along to ensure that they are adapting and utilizing these new capabilities. This is partly what oversight is about—constant hearings, and updates—pushing this wherever possible. As is understanding the lay of the land, understanding our adversaries' capabilities and investments—if they are trying to counter our advantage—or trying to invest in new technology areas that we may have ignored.

One of the things that comes to mind is our electronic warfare and how the United States' EW capabilities have somewhat atrophied. The Pentagon recognizes this and has revitalized its efforts to understand the nature of our EW challenges and what the United States needs to do on the defensive and offensive levels. Additionally, the Pentagon is making those changes and those investments known.

Are additional reforms needed within the Defense Department?

It is important to note that the past two National Defense Authorization Acts have contained key reforms that will require time for implementation. Separating research and development programs from acquisitions was key. We also elevated U.S. Cyber Command to a unified combatant command. There is still a question as to whether USCYBERCOM and the NSA should be split. At this point, I am not prepared to say USCYBERCOM should be split. How and when to end the dual-hat arrangement is a question we will have to grapple with down the road.