By Steven Beardsley

MUNICH, Germany — The concept of cyberwar crossed a threshold in 2010, says Michael Hayden, former CIA and NSA director, when the Stuxnet computer worm destroyed a series of nuclear centrifuges in Iran by hijacking their controls.

Where previous notable cyber attacks had disrupted systems, Stuxnet destroyed property — it was a cyberweapon, Hayden said at the close of the annual Munich Security Conference Sunday.

Hayden and other experts in cybersecurity agreed that the dangers of such weapons remain high in a world of networked infrastructure, and tracking attackers is especially difficult.

The conference comes as the U.S. Defense Department considers the best response to cyber attacks that could cripple critical U.S. infrastructure, including utilities. Last May, the DOD made news when officials said a lethal, real-world attack could be used in response.

For Estonian President Toomas Hendrick Ilves, a participant in Sunday's panel, such retaliation is appropriate. Estonian government servers fell victim to a broadly distributed denial-of-service attack in 2007, that crippled state websites and some state functions. The attack taught him a lesson about civil society's reliance on networking, down to the delivery of basic needs.

"You don't have to have a missile," Ilves said. "You don't even have to shut down a centrifuge. You can just play around with a delivery system, and no milk is there."

Yet one of the cyber domain's key attributes, it's anonymity, makes retaliation difficult. Blame in the Estonia attacks was eventually attributed to a group of pro-Russian sources that some term "hacktivists." Likewise, the origin of Stuxnet was never pinpointed.

Eugene Kaspersky, chairman and CEO of a private lab that works in cybersecurity, expressed concern that more "hacktivists" would seek cyber weapons like Stuxnet and become cyberterrorists. A flaw in the use of the Stuxnet is that much of its coding remained visible to its victims, allowing the worm to be modified and perpetuated.

"This is why I say, stop the use of cyberweapons, Kaspersky said. "If you use it, you educate your enemies. And this boomerang will get back to you."

Such cyber weapons can also cause havoc when improperly programmed, Kaspersky said. A worm aimed at one piece of infrastructure can carry far-reaching consequences to other networks if not directed properly, he said. The panel struggled with the dilemma of controlling the use and development of such weapons in a world where billions of people are tethered to the Internet. While increased interconnectivity raises the stakes of cyberwar, restriction on the Internet is often seen as inhibiting freedom of expression, panelists said.

"We would make a fundamental mistake, even in the name of security to restrict it," Italian Defense Minister Giampaolo Di Paola said. "We have to learn to regulate it and raise awareness of its importance in the global economy."

Hayden said the U.S. is still grappling with cybersecurity versus cyberfreedom.

"This is a policy desert for us," he said. "We lack legal and policy guidance for what we expect the government to do."

Original article on the Stars and Stripes webpage .