'Tallinn Manual 2.0'—the rulebook for cyberwar
3 June 2017, by Michel Moutot

Launched in 2009, the annual event is organised by NATO's Cooperative Cyber Defence Centre of Excellence based in the Estonian capital.

In 2007, Estonia was among the first countries to suffer a massive cyber attack, with authorities in Tallinn blaming the Baltic state's Soviet-era master Russia.

"The very next year, in the war between Russia and Georgia, again we saw a lot of cyber activity," said Schmitt, speaking to AFP at Cycon.

Estonia was targeted just three years after it joined NATO and the EU in 2004.

The attack raised a slew of serious questions about how to apply and enforce NATO's Article 5 collective defence guarantee in cyberspace, said Schmitt, who also chairs the Stockton Center for the Study of International Law at the United States Naval War College.

He said that NATO allies faced an unprecedented dilemma: did the attack "mean that NATO states had to somehow come to the rescue of Estonia or not?"

Was it "an attack on the civilian population, a violation of international humanitarian law or not? No one had the answers," he added.

"Because of that (attack) the international community started looking at cyber, going: 'Oh my God, I can't answer any question!' That's why this manual was started."

'Digital wild west'

Schmitt says his team's work is intended to tame the "digital wild west" that emerged with the advent of cyberspace.

But the virtually limitless range of possibilities in
cyber-conflict raises a long laundry list of legal questions and dilemmas and the Tallinn Manual certainly cannot answer them all.

The legal experts, mostly professors of international law, filled its 642 pages with existing jurisprudence applying to cyberspace from across the globe, and did not shy away from laying out conflicting views on certain issues.

For example: should cyber-espionage be subject to the same laws as conventional spying? Can a state obtain the online IDs and passwords of prisoners of war and use them?

Does a cyberattack trigger a legitimate right to self-defence? Can you retaliate? What kind of status do victims have? What can you do when there is no evidence to prove guilt when attackers can easily cover their tracks?

"This book is intended to be a secondary source of law: it explains the law, but it doesn't create it. States make law," Schmitt told AFP.

"My goal is that this books sits on the desk of every legal advisor for defence and foreign ministers, the intelligence services, so that legal advisors can sit with policy makers and say: in this situation, we can do this, or the law is not clear, you need to make a political decision here.

"But at least the discussion is mature. It's not 'oh my God, what's happening to us?'."

© 2017 AFP


This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.