SPIEGEL ONLINE

04/04/2013 06:06 PM

Arming for Virtual Battle

The Dangerous New Rules of Cyberwar

By Thomas Darnstaedt, Marcel Rosenbach and Gregor Peter Schmitz

Now that wars are also being fought on digital battlefields, experts in international law have established rules for cyberwar. But many questions remain unanswered. Will it be appropriate to respond to a cyber attack with military means in the future?

The attack came via ordinary email, when selected South Korean companies received messages supposedly containing credit card information in the middle of the week before last.

Recipients who opened the emails also opened the door to the enemy, because it was in fact an attack from the Internet. Instead of the expected credit card information, the recipients actually downloaded a time bomb onto their computers, which was programmed to ignite on Wednesday at 2 p.m. Korean time.

At that moment, chaos erupted on more than 30,000 computers in South Korean television stations and banks. The message "Please install an operating system on your hard disk" appeared on the screens of affected computers, and cash machines ceased to operate. The malware, which experts have now dubbed "DarkSeoul," deleted data from the hard disks, making it impossible to reboot the infected computers.

DarkSeoul was one of the most serious digital attacks in the world this year, but cyber defense centers in Western capitals receive alerts almost weekly. The most serious attack to date originated in the United States. In 2010, high-tech warriors, acting on orders from the US president, smuggled the destructive "Stuxnet" computer worm into Iranian nuclear facilities.

The volume of cyber attacks is only likely to grow. Military leaders in the US and its European NATO partners are outfitting new battalions for the impending data war. Meanwhile, international law experts worldwide are arguing with politicians over the nature of the new threat. Is this already war? Or are the attacks acts of sabotage and terrorism? And if a new type of war is indeed brewing, can military means be used to respond to cyber attacks?

The War of the Future

A few days before the computer disaster in Seoul, a group led by NATO published a thin, blue booklet. It provides dangerous responses to all of these questions. The "Tallinn Manual on the International Law Applicable to Cyber Warfare" is probably no thicker than the American president's thumb. It is not an official NATO document, and yet in the hands of President Barack Obama it has the potential to change the world.

The rules that influential international law experts have compiled in the handbook could blur the lines between war and peace and allow a serious data attack to rapidly escalate into a real war with bombs and missiles. Military leaders could also interpret it as an invitation to launch a preventive first strike in a cyberwar.

At the invitation of a NATO think tank in the Estonian capital Tallinn, and at a meeting presided over by a US military lawyer with ties to the Pentagon, leading international law experts had discussed the rules of the war of the future. International law is, for the most part, customary law. Experts determine what is and can be considered customary law.

The resulting document, the "Tallinn Manual," is the first informal rulebook for the war of the future. But it has no reassuring effect. On the contrary, it permits nations to respond to data attacks with the weapons of real war.

Two years ago, the Pentagon clarified where this could lead, when it stated that anyone who attempted to shut down the electric grid in the world's most powerful nation with a computer worm could expect to see a missile in response.

A Private Digital Infrastructure

The risks of a cyberwar were invoked more clearly than ever in Washington in recent weeks. In mid-March, Obama assembled 13 top US business leaders in the Situation Room in the White House basement, the most secret of all secret conference rooms. The group included the heads of UPS, JPMorgan Chase and ExxonMobil. There was only one topic: How can America win the war on the Internet?

The day before, Director of National Intelligence James Clapper had characterized the cyber threat as the "biggest peril currently facing the United States."

The White House was unwilling to reveal what exactly the business leaders and the president discussed in the Situation Room. But it was mostly about making it clear to the companies how threatened they are and strengthening their willingness to cooperate, says Rice University IT expert Christopher Bronk.

The president urgently needs their cooperation, because the US has allowed the laws of the market to govern its digital infrastructure. All networks are operated by private companies. If there is a war on the Internet, both the battlefields and the weapons will be in private hands.

This is why the White House is spending so much time and effort to prepare for possible counterattacks. The aim is to scare the country's enemies, says retired General James Cartwright, author of the Pentagon's current cyber strategy.

Responsible for that strategy is the 900-employee Cyber Command at the Pentagon, established three years ago and located in Fort Meade near the National Security Agency, the country's largest intelligence agency. General Keith Alexander heads both organizations. The Cyber Command, which is expected to have about 4,900 employees within a few years, will be divided into various defensive and offensive "Cyber Mission Forces" in the future.

Wild West Online

It's probably no coincidence that the Tallinn manual is being published now. Developed under the leadership of US military lawyer Michael Schmitt, NATO representatives describe the manual as the "most important legal document of the cyber era."

In the past, Schmitt has examined the legality of the use of top-secret nuclear weapons systems and the pros and cons of US drone attacks. Visitors to his office at the Naval War College in Rhode Island, the world's oldest naval academy, must first pass through several security checkpoints.

"Let's be honest," says Schmitt. "Everyone has treated the Internet as a sort of Wild West, a lawless zone. But international law has to be just as applicable to online weapons as conventional weapons."

It's easier said than done, though. When does malware become a weapon? When does a hacker become a warrior, and when does horseplay or espionage qualify as an "armed attack," as defined under international law? The answers to such detailed questions can spell the difference between war and peace.

James Lewis of the Washington-based Center for Strategic and International Studies (CSIS), one of the country's top cyberwar experts, is somewhat skeptical about the new manual. He sees it as "a push to lower the threshold for military action." For Lewis, responding to a "denial of service" attack with military means is "really crazy." He says the Tallinn manual "shows is that you should never let lawyers go off by themselves."

Claus Kress, an international law expert and the director of the Institute for International Peace and Security Law at the University of Cologne, sees the manual as "setting the course," with "consequences for the entire law of the use of force." Important "legal thresholds," which in the past were intended to protect the world against the military escalation of political conflicts or acts of terror, are becoming "subject to renegotiation," he says.

According to Kress, the most critical issue is the "recognition of a national right of self-defense against certain cyber attacks." This corresponds to a state of defense, as defined under Article 51 of the Charter of the United Nations, which grants any nation that becomes the victim of an "armed attack" the right to defend itself by force of arms. The article gained new importance after Sept. 11, 2001, when the US declared the invasion of Afghanistan an act of self-defense against al-Qaida and NATO proclaimed the application of its mutual defense clause to come to the aid of the superpower.

Changing the Logic of War

The question of how malicious malware must be to justify a counterattack can be critical when it comes to preserving peace. Under the new doctrine, only those attacks that cause physical or personal damage, but not virtual damage, are relevant in terms of international law. The malfunction of a computer or the loss of data alone is not sufficient justification for an "armed attack."

But what if, as is often the case, computer breakdowns do not result in physical damage but lead to substantial financial losses? A cyber attack on Wall Street, shutting down the market for several days, was the casus belli among the experts in Tallinn. The US representatives wanted to recognize it as a state of defense, while the Europeans preferred not to do so. But the US military lawyers were adamant, arguing that economic damage establishes the right to launch a counterattack if it is deemed "catastrophic."

Ultimately, it is left to each country to decide what amount of economic damage it considers sufficient to venture into war. German expert Kress fears that such an approach could lead to a "dam failure" for the prohibition of the use of force under international law.

So was it an armed attack that struck South Korea on March 20? The financial losses caused by the failure of bank computers haven't been fully calculated yet. It will be up to politicians, not lawyers, to decide whether they are "catastrophic."

Just how quickly the Internet can become a scene of massive conflicts became evident this month, when suddenly two large providers came under constant digital attack that seemed to appear out of nowhere.

The main target of the attack was the website Spamhaus.org, a project that has been hunting down the largest distributors of spam on the Web since 1998. Its blacklists of known spammers enable other providers to filter out junk email. By providing this service, the organization has made powerful enemies and has been targeted in attacks several times. But the current wave of attacks overshadows everything else. In addition to shutting down Spamhaus, it even temporarily affected the US company CloudFlare, which was helping fend off the attack. Analysts estimate the strength of the attack at 300 gigabits per second, which is several times as high as the level at which the Estonian authorities were "fired upon" in 2007. The attack even affected data traffic in the entire Internet. A group called "Stophaus" claimed responsibility and justified its actions as retribution for the fact that Spamhaus had meddled in the affairs of powerful Russian and Chinese Internet companies.

Civilian forces, motivated by economic interests, are playing cyberwar, and in doing so they are upending all previous war logic.

A Question of When, Not If

A field experiment in the US shows how real the threat is. To flush out potential attackers, IT firm Trend Micro built a virtual pumping station in a small American city, or at least it was supposed to look like one to "visitors" from the Internet. They called it a "honeypot," designed to attract potential attackers on the Web.

The trappers installed servers and industrial control systems used by public utilities of that size. To make the experiment setup seem realistic, they even placed deceptively real-looking city administration documents on the computers.

After only 18 hours, the analysts registered the first attempted attack. In the next four weeks, there were 38 attacks from 14 countries. Most came from computers in China (35 percent), followed by the US (19 percent) and Laos (12 percent).

Many attackers tried to insert espionage tools into the supposed water pumping station to probe the facility for weaknesses. International law does not prohibit espionage. But some hackers went further than that, trying to manipulate or even destroy the control devices.

"Some tried to increase the rotation speed of the water pumps to such a degree that they wouldn't have survived in the real world," says Trend Micro employee Udo Schneider, who categorizes these cases as "classic espionage."

"There is no question as to whether there will be a catastrophic cyber attack against America. The only question is when," says Terry Benzel, the woman who is supposed to protect the country from such an attack and make its computer networks safer. The computer specialist is the head of DeterLab in California, a project that was established in 2003, partly with funding from the US Department of Homeland Security, and offers a simulation platform for reactions to cyber attacks.

Benzel's voice doesn't falter when she describes a war scenario she calls "Cyber Pearl Harbor." This is what it could look like: "Prolonged power outages, a collapse of the power grid and irreparable disruptions in the Internet." Suddenly, food would not reach stores in time and cash machines would stop dispensing money. "Everything depends on computers nowadays, even the delivery of rolls to the baker around the corner," she says.

Benzel also describes other crisis scenarios. For example, she says, there are programs that open and close gates on American dams that are potentially vulnerable. Benzel is worried that a clever hacker could open America's dams at will.

Should Preemptive Strikes Be Allowed?

These and other cases are currently being tested in Cyber City, a virtual city US experts have built on their computers in New Jersey to simulate the consequences of data attacks. Cyber City has a water tower, a train station and 15,000 residents. Everything is connected in realistic ways, enabling the experts to study the potentially devastating effects cyber attacks could have on residents.

In Europe, it is primarily intelligence agencies that are simulating digital war games. Germany's foreign intelligence service, the *Bundesnachrichtendienst* (BND), also has a unit that studies the details of future wars. It is telling that the BND team doesn't just simulate defensive situations but increasingly looks at offensive scenarios, as well, so as to be prepared for a sort of digital second strike.

"Offensive Cyber Operations," or OCOs, are part of the strategy for future cyberwars in several NATO countries. The Tallinn manual now establishes the legal basis for possible preemptive strikes, which have been an issue in international law since former US President George W. Bush launched a preemptive strike against Iraq in March 2003.

The most contentious issue during the meetings in Tallinn was the question of when an offensive strike is permissible as an act of preventive self-defense against cyber attacks. According to the current doctrine, an attack must be imminent to trigger the right to preventive self-defense. The Tallinn manual is more generous in this respect, stating that even if a digital weapon is only likely to unfold its sinister effects at a later date, a first strike can already be justified if it is the last window of opportunity to meet the threat.

The danger inherent in the application of that standard becomes clear in the way that the international law experts at Tallinn treated Stuxnet, the most devastating malware to date, which was apparently smuggled into Iranian nuclear facilities on Obama's command. The data attack destroyed large numbers of centrifuges used for uranium enrichment in the Natanz reprocessing plant. Under the criteria of the Tallinn manual, this would be an act of war.

Could the US be the perpetrator in a war of aggression in violation of international law? Cologne international law expert Kress believes that what the Tallinn manual says parenthetically about the Stuxnet case amounts to a "handout for the Pentagon," namely that Obama's digital attack might be seen as an "act of preventive self-defense" against the nuclear program of Iran's ayatollahs.

The Fog of Cyber War

According to the Tallinn interpretation, countless virtual espionage incidents of the sort that affect all industrialized nations almost daily could act as accelerants. Pure cyber espionage, which American politicians also define as an attack, is not seen an act of war, according to the Tallinn rules. Nevertheless, the international law experts argue that such espionage attacks can be seen as preparations for destructive attacks, so that it can be legitimate to launch a preventive attack against the spy as a means of self-defense.

Some are especially concerned that the Tallinn proposals could also make it possible to expand the rules of the "war on terror." The authors have incorporated the call of US geostrategic expert Joseph Nye to take precautions against a "cyber 9/11" into their manual. This would mean that the superpower could even declare war on organized hacker groups. Combat drones against hackers? Cologne expert Kress cautions that the expansion of the combat zone to the laptops of an only loosely organized group of individuals would constitute a "threat to human rights."

Germany's military, the Bundeswehr, is also voicing concerns over the expansion of digital warfare. Karl Schreiner, a brigadier general with the Bundeswehr's leadership academy in Hamburg, is among those who see the need for "ethical rules" for the Internet battlefield and believe that an international canon for the use of digital weapons is required.

Military leaders must rethink the most important question relating to defense in cyberspace: Who is the attacker? "In most cases," the Tallinn manual reads optimistically, it is possible to identify the source of data attacks. But that doesn't coincide with the experiences of many IT security experts.

The typical fog of cyberwar was evident most recently in the example of South Korea. At first, officials said that DarkSeoul was clearly an attack from the north, but then it was allegedly traced to China, Europe and the United States. Some analysts now suspect patriotically motivated hackers in North Korea, because of the relatively uncomplicated malware. That leaves the question of just who South Korea should launch a counterattack against.

The South Korean case prompts Cologne international law expert Kress to conclude that lawyers will soon have a "new unsolved problem" on their hands -- a "war on the basis of suspicion."

Translated from the German by Christopher Sultan

URL:

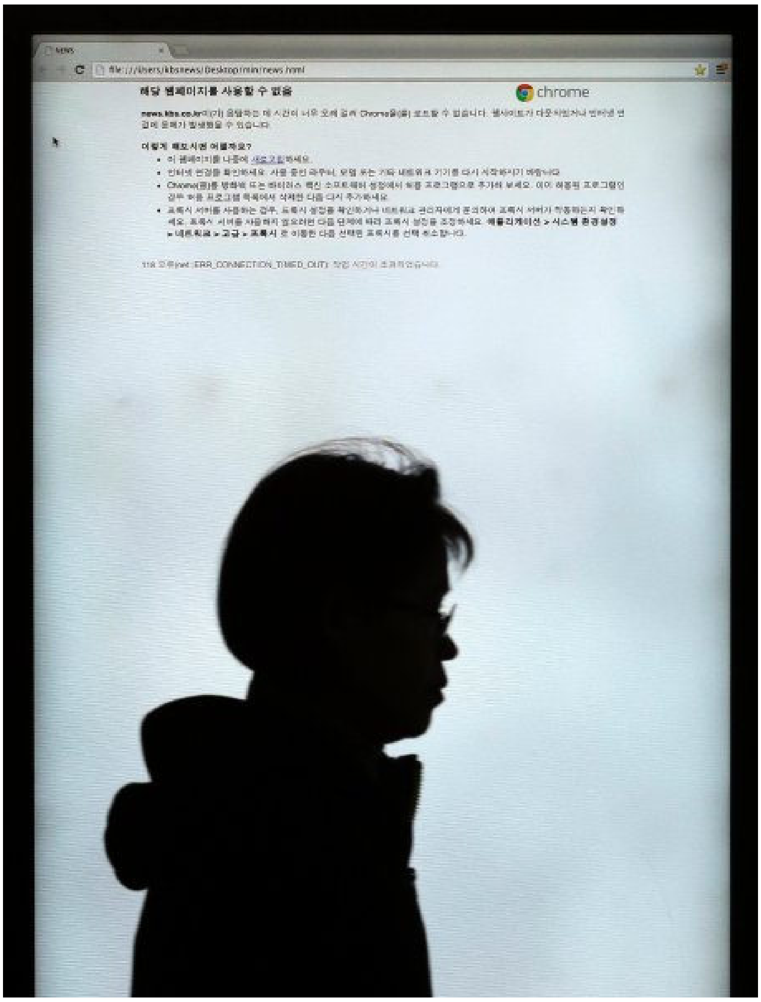
- http://www.spiegel.de/international/world/expanding-combat-zone-the-dangerous-new-rules-of-cyberwar-a-892238.html

Related SPIEGEL ONLINE links:

- Cyber Menace: Digital Spying Burdens German-Chinese Relations (02/25/2013) http://www.spiegel.de/international/world/0,1518,885444,00.html
- The Hunt for Red October: Virus Hunters Try to Catch Diplomatic Time Bomb (01/25/2013) http://www.spiegel.de/international/spiegel/0,1518,879467,00.html
- Unknown But Unavoidable: The Secret Ways of Chinese Telecom Giant Huawei (01/02/2013) http://www.spiegel.de/international/business/0,1518,875297,00.html

UNITED STATES CYBER COMMAND

CSIS
CENTER FOR STRATEGIC & INTERNATIONAL STUDIES
ALEXANDER


NEWS
file:///Users/kbsnews/Desktop/min/news.html
해당 웹페이지를 사용할 수 없음
chrome
어떻게 해보시면 어떨까요?
118 오류(net::ERR_CONNECTION_TIMED_OUT): 작업 시간이 초과되었습니다.