Cyber attacks 10 years on—from disruption to disinformation

April 27 2017, by Tom Sear

The solider of Tallinin, a bronze statue that triggered the first recognised cyber attack. Credit: 65817306@N00/flickr , CC BY-NC

Today is the tenth anniversary of the world's first major coordinated "cyber attack" on a nation's internet infrastructure. This little-known event set the scene for the onrush of cyber espionage, fake news and information wars we know today.

In 2007, operators took advantage of political unrest to unleash a series

of cyber measures on Estonia, as a possible form of retribution for symbolically rejecting a Soviet version of history. It was a new, coordinated approach that had never been seen before.

Today, shaping contemporary views of historical events is a relatively common focus of coordinated digital activity, such as China's use of social media to create war commemoration and *Russia Today*'s live-tweeting the Russian Revolution as its centenary approaches.

> A comrade just called me the 'Father of All Bolsheviks'. Well, who is the 'Mother of All Bolsheviks' then? #MOAB #FOAB #1917LIVE
>
> — Vladimir Lenin (@VLenin_1917) April 14, 2017

In 2017 and into the future, it will be essential to combine insights from the humanities, particularly from history, with analysis from information operations experts in order to maintain cyber security.

Estonia ground to a halt

A dispute over a past war triggered what might be called the first major "cyber attack".

On April 27, 2007 the Government of Estonia moved the "Soldier of Tallinn" – a bronze statue that commemorated the Soviet Army of World War II – from the centre of the city to a military cemetery on Tallinn's outskirts. The action followed an extensive debate over the interpretation of Estonia's past. A "history war" concerning the role of the Soviet Union in Estonia during and after World War II had split Estonian society.

Several days of violent confrontation followed the statue's removal. The

Russian-speaking population rioted. The protests led to 1,300 arrests, 100 injuries and one death. The disturbance became known as "Bronze Night".

A more serious disruption followed, and the weapons were not Molotov cocktails, but thousands of computers. For almost three weeks, a series of massive cyber operations targeted Estonia.

The disruption – which peaked on May 9 when Moscow celebrates Victory Day – brought down banks, the media, police, government networks and emergency services. Bots, distributed denial-of-service (DDoS) and spam were marshalled with a sophistication not seen before. Their combined effects brought one of the most digital-reliant societies in the world to a grinding halt.

The Tallinn Manual

In the aftermath, NATO responded by developing the NATO Cooperative Cyber Defence Centre of Excellence in Estonia. A major contribution of the centre was the publication of the Tallinn Manual in 2013 – a comprehensive study of how international law applied to cyber conflict. The initial manual focused on disabling, state-based attacks that amount to acts of war.

Tallinn 2.0 was released in February 2017. In the foreword, Estonian politician Toomas Hendrik Ives argues:

In retrospect, these were fairly mild and simple DDoS attacks, far less damaging than what has followed. Yet it was the first time one could apply the Clausewitzean dictum: War is the continuation of policy by other means.

The focus of the new manual reveals just how much the world of cyber

operations has changed in the ten years since Bronze Night. It heralds a concerning future where all aspects of society, not just military and governmental infrastructure, are subject to active cyber operations.

Now the scope for digital incursions by one nation on another is much wider, and more widespread. Everything from the personal data of citizens held in government servers to digitised cultural heritage collections have become issues of concern to international cyber law experts.

A decade of cyber operations

In the ten years since 2007 we have lived in an era where persistent cyber operations are coincident with international armed combat. The conflict between Georgia (2008) and Russia, and ongoing conflict in the Ukraine (since 2014) are consistent with this.

These operations have extended beyond conventional conflict zones via intrusion of civic and governmental structures.

There are claims of nation-state actors active measures and DDoS incidents (similar to those that may have disabled last year's Australian census) on Kyrgyzstan and Kazakhstan in 2009.

German investigators found a penetration of the Bundestag in May 2015.

The Dutch found penetration in government computers relating to MH17 reports.

Now, famously, we know there were infiltrations between 2015-16 into US Democratic party computers. Revealed in the last few days, researchers have identified phishing domains targeting French political campaigns.

There are even concerns that, as Professor Greg Austin has explained, cyber espionage might be a threat to Australian democracy.

Recently, the digital forensics of a computer hacked in 1998 as part of an operation tagged Moonlight Maze revealed that it is possible that the same code and threat actor have been involved in operations since at least that time. Perhaps a 20-year continuous cyber espionage campaign has been active.

Thomas Rid, Professor in Security Studies at King's College London, recently addressed the US Select Committee on Intelligence regarding Russian active measures and influence campaigns. He expressed his opinion that understanding cyber operations in the 21st century is impossible without first understanding intelligence operations in the 20th century. Rid said:

This is a field that's not understanding its own history. It goes without saying that if you want to understand the present or the future, you have to understand the past.

Targeting information and opinion

Understanding the history of cyber operations will be critical for developing strategies to combat them. But narrowly applying models from military history and tactics will offer only specific gains in an emerging ecosystem of "information age strategies".

The international response to the "attack" on Estonia was to replicate war models of defence and offence. But analysis of the last ten years shows that is not the only way in which cyber conflict has evolved. Even the popular term "cyber attack" is now discouraged for incidents smaller than Estonia, as risks on the cyber security spectrum have become more complex and more precisely defined.

Since Estonia 2007, internet-based incursions and interference have escalated massively, but their targets have become more diffuse. Direct attacks on a nation's defence forces, while more threatening, may in the future be less common than those that target information and opinion.

At the time, the attack on national infrastructure in Estonia seemed key, but looking back it was merely driving a wedge into an existing polarisation in society, which seems to be a pivotal tactic.

Nations like Australia are more vulnerable than ever to cyber threats, but their public focus is becoming more distributed, and their goal will be to change attitudes, opinions and beliefs.

A decade ago in Estonia, a cyber war erupted from a history war. The connection between commemoration and information war is stronger than ever, and if nations wish to defend themselves, they will need to understand culture as much as coding.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

Citation: Cyber attacks 10 years on—from disruption to disinformation (2017, April 27) retrieved 2 May 2024 from
https://phys.org/news/2017-04-cyber-years-onfrom-disruption-todisinformation.html