RSIS COMMENTARIES (43/2007)

RSIS Commentaries are intended to provide timely and, where appropriate, policy relevant background and analysis of contemporary developments. The views of the authors are their own and do not represent the official position of the S.Rajaratnam School of International Studies, NTU.

The First Information War?
Russia's Cyberwar Against Estonia

Paul T. Mitchell[*]

23 May 2007

IN APRIL, the tiny Baltic state of Estonia moved a war memorial dedicated to fallen Soviet soldiers of World War Two from its prominent location in central Tallin to a military cemetery outside the capital. The act resulted first in a series of civil disturbances throughout the ethnically-diverse country that left one dead, 40 injured, and 300 arrested. However, it is the subsequent "cyber-war", ostensibly lead by the Kremlin, that has attracted the most attention in recent days. The media has typically warned of new forms of warfare that threaten modern societies, however, there is much that is familiar in the present conflict. Overlooked is the role that Estonia has played in recent months to frustrate a German/Russian oil pipeline. Indeed, Germany's Gerhard Schroeder recently claimed that in this dispute Estonia had contradicted "every form of civilised behaviour".

A playback of history

For all the sound and light accompanying the story, the context is depressingly familiar for students of history. Indeed, the story is at least as old as the Peloponnesian war. In 416BC, the superpower of the age, maritime Athens demanded the obeisance of the tiny neutral republic of Melos with the famous observation that "the strong do what they can and the weak suffer what they must". Russia seems intent of reminding Estonia, now emboldened by membership in both NATO and the European Union (EU), of this eternal strategic truth.

In times past, the Kremlin might have had to content itself with massing tank armies on the border of Estonia. Such sabre-rattling would have led to a significant crisis in East-West relations that had a high potential of cascading out of control. Information Technology (IT) gives actors of all stripes new avenues for coercion, especially of "fragile" modern societies like Estonia. John Robb, the author of *Brave New War* points to the ability of "global guerrillas" to create systemic disruptions with IT by attacking the infrastructure of a country. Estonia is highly vulnerable to such attacks. Most of its government provides services through on-line portals, and its banking sector is heavily dependent on on-line services. While Robb is primarily concerned with the actions of groups like Al Qaeda, clearly these capabilities are well within the ambit of states as well.

Russian targets

To date, cyber attacks on Estonia have been limited to denial of service attacks (DOS). Websites for the Estonian presidency, its parliament, government ministries and political parties have all been targeted, as have three of the six news agencies and two of its banks. Given the role of the Internet in facilitating Estonian elections, such attacks are clearly worrisome in their potential impacts. Initial attacks were poorly executed, reportedly from computers traceable to the Kremlin itself. However, later attacks emerged from a wide variety of international sources, probably from “zombie” systems. So called “bot-nets” are built from a series of remote computers that, without the owner’s knowledge, overwhelm targeted web-sites with waves of spam or information requests. Such zombies are recruited through the spread of viruses or Trojan horses onto the affected systems. As these attacks have come from systems as far away as Vietnam, Estonia has had to block many of its sites to international traffic, impacting especially the conduct of on-line business.

As disruptive as DOS is for websites providing information and services, it is important to note that such disruptions are more of an irritant than anything else. DOS attacks against on-line banking services and businesses are certainly a modern form of economic warfare resulting in lost income and as such must be considered seriously. However, the effective collapse of Estonia’s economy would probably require a long term sustained campaign that the present underground methods are unlikely to deliver, especially given the growing support being provided to Estonia from NATO computer security experts. For example, consider how ineffective much more comprehensive sanctions regimes targeting Serbia, Iraq, and other pariah states have been in gaining political compliance.

What next?

More pernicious forms of information warfare may yet surface in this current struggle. As yet, however, there have been no reports of the alteration of information on secure websites, or the collapse of public services such as energy, communication and transportation networks. States may be reluctant to engage in such tactics given the efficacy of reciprocal use against the attacker. Indeed, in past conflicts, the US has refrained from engaging these forms of information warfare for fear of breaching these operational taboos.

While many in the media are calling this the first information war, the coercive use of IT is at least a decade old. The *Guardian* reported that the US allegedly used “offensive hacking” against Haiti in 1995. Furthermore, Serbia engaged in information warfare against both NATO and the US during the Kosovo conflict in 1999. The Serbs shut down NATO web servers using DOS attacks, and managed to hack into secure sites, defacing them with their own propaganda. The Serbs even managed to crash a White House server. The US reportedly feared being accused of war crimes if they attacked “civilian” web sites. Since these early campaigns, however, information warfare has become increasingly ubiquitous. Last year, Hizbullah used Photo-Shopped .jpg files for propaganda purposes as an important tool to shape international opinion of Israeli operations. The website infowar-monitor.net currently watches the coercive use of IT in five different conflict areas, including Chechnya, and India-Pakistan.

So is anything new in this current struggle? The bot-net nature of the conflict points to the creative use of the anarchical features of the Internet itself. One Estonian computer security specialist noted that “the EU and NATO need to work out a common legal basis to deal with cyber-attacks”, as if this were some minor bureaucratic misunderstanding.

Implications of the cyberwar

This misses the whole point that using distributed attacks from anonymous zombie systems, Russia gains enough plausible deniability to frustrate any legal challenge until long after the political effect of such attacks have already had their impact. However, much of this present conflict is fairly well grounded in historical precedent. The small nation of Estonia, with as much as 40% of its population being ethnic Russian, has unwisely provoked its much larger neighbour and now must hope that the thin promises of collective defence enshrined in

Article V of the Washington Treaty will be enough to protect its sovereignty. In the 1939 Winter War, Finland played a very similar game against Russia and lost; most of Scandinavia took notice, going to extreme lengths to avoid angering the Russian bear even during the height of the Cold War.

Information technology clearly gives Estonia some resources to play against the Russians in this struggle. An effective counter-information campaign is beginning to emerge in the very nature of the Western media's coverage of this skirmish. Further, just as smaller Hizbullah was able to manipulate an ironic "David vs. Goliath" image, so too can Western Estonia confront the traditional Eastern Russian bully. However, none of this changes the fundamental strategic logic of geographical proximity. In the end, Brussels is much further removed from Tallin than Moscow. Estonia will not be deprived of its sovereignty by DOS attacks, but rather through a sustained campaign against its infrastructure and the removal of its government's ability to control its own territory. Info-war may play a role in this, but it will not remove the need for the ubiquitous "boots on the ground".

[*] *Paul T. Mitchell is an Associate Professor with the Revolution in Military Affairs (RMA) Programme of the S. Rajaratnam School of International Studies, NTU.*