Marching off to cyberwar

economist.com
Dec 4th 2008

AS RUSSIAN tanks rolled into Georgia in August, another force was also mobilising—not in the physical world, but online. Russian nationalists (or indeed anyone else) who wished to take part in the attack on Georgia could do so from anywhere with an internet connection, simply by visiting one of several pro-Russia websites and downloading the software and instructions needed to perform a “distributed denial of service” (DDoS) attack. This involves sending a flood of bogus requests to an internet server, so that it is overwhelmed by the demand and becomes unusable.

One website, called StopGeorgia, provided a utility called DoSHTTP, plus a handy list of target websites, including those of Georgian government agencies and the British and American embassies in the capital, Tbilisi. Launching an attack was as simple as entering the address and clicking a button labelled “Start Flood”. The StopGeorgia website helpfully indicated which target sites were still active and which had collapsed under the weight of bogus requests. Other websites explained how to write simple programs to send a flood of requests, or offered specially formatted webpages that could be set to reload themselves continuously, deluging particular Georgian websites with traffic.
The actual damage done was minimal: some e-mail was disrupted and some target sites were rendered unavailable to the public. The cyberattacks on Estonia in 2007, also launched from Russia, were more effective because Estonia’s government relies far more heavily on the internet (its parliament declared internet access a human right in 2000). They briefly upset the operations of some government organisations, including telephone access to the emergency services.

There is no conclusive evidence that either set of attacks was executed or sanctioned by the Russian government—though there is no evidence that it tried to stop them, either. Ethan Zuckerman, an internet expert at Harvard, has described the plethora of competing theories as “the fog of cyberwar”. And in the Georgian case volunteer cyberwarriors—dubbed “a citizen DDoS army” by Artem Dinaburg of Damballa, a cybersecurity start-up—were also involved. Does any of this really count as an act of war? The Estonian and Georgian cyberattacks have put to the test a host of theories about cyberwarfare: how to define it; whether to engage in it; and how to defend against it.

A definition of war

The discussion of cyberattacks and cyberwarfare is complicated by widespread disagreement over how to define these terms. Many cyberattacks are really examples of vandalism or hooliganism, observes Bruce Schneier, a security guru who works for BT, a British telecoms operator. A cyberattack on a power station or an emergency-services call centre could be an act of war or of terrorism, depending on who carries it out and what their motives are.

For a cyberattack to qualify as “cyberwar”, some observers argue, it must take place alongside actual military operations. Trying to disrupt enemy communications during conflict is, after all, a practice that goes back to the earliest telecommunications technology, the telegraph. In 1862, for example, during the American Civil War, a landing party from Thomas Freeborn, a Union navy steamer, went ashore to cut the telegraph lines between Fredericksburg and Richmond. The Russian navy pioneered the use of radio jamming in the Russo-Japanese war of 1905. On this view, cyberattacks on infrastructure are the next logical step. The attacks on Georgia might qualify as cyberwarfare by this definition, but those on Estonia would not, since there was no accompanying military offensive in the real world. As Mr Schneier puts it: “For it to be cyberwar, it must first be war.”

Not everyone agrees. For years there has been talk of a “digital Pearl Harbour”—an
unexpected attack on a nation’s infrastructure via the internet, in which power stations are shut down, air-traffic control is sabotaged and telecoms networks are disabled. There have even been suggestions that future wars could be waged in cyberspace, displacing conventional military operations altogether. Why bomb your enemy’s power-stations or stockmarkets if you can disable them with software? So far there have been no successful attacks of this type, but that does not stop people worrying about them—or speculating about how to launch them.

The strongest definition of cyberwar requires that cyberattacks cause widespread harm, rather than mere inconvenience. The Georgian attacks did not cause physical harm, unlike the military operations going on at the same time.

Such definitions matter because cybervandalism or cyberhooliganism are forms of cybercrime, which (in theory at least) is dealt with by various national and international law-enforcement agencies according to existing legal conventions, such as the Council of Europe Convention on Cybercrime. A private individual in Russia who defaces an Estonian website ought to be treated in a similar fashion to his neighbour who travels to Tallinn, breaks a shop window and goes into hiding in Russia—though identifying a cyberattacker is far from easy and after the attacks in 2007 the Russian authorities refused to co-operate with Estonian investigators.

Such was the intensity of the attacks on Estonian websites, however, that the country’s defence minister, Jaak Aaviksoo, warned that the action “cannot be treated as hooliganism, but has to be treated as an attack against the state”. But treating the attacks as acts of war would mean applying a different set of rules, presenting a new challenge to policymakers.

All sorts of “translation problems” arise when trying to apply existing international rules relating to terrorism and warfare to online attacks, says Duncan Hollis, a professor of law at Temple University in Pennsylvania. The United Nations Charter prohibits the use of force except when authorised by the Security Council, for example, but does not spell out what counts as “the use of force” in cyberspace. Do DDoS attacks count? Perhaps not if aimed at a newspaper website, but what about an air-traffic control system?

Agreement on a definition is needed, says Mr Hollis, because under international law a country that considers itself the victim of an act of war has the right to self-defence—with conventional military (not merely electronic) means. And members of an alliance with mutual-defence obligations, such as NATO, may be duty-bound to respond to an attack on
any of their members. So the cyberattack on Estonia, a NATO member, could in theory have prompted a military response. To grapple with questions like these, and to bring together a group of experts in “cyberdefence”, NATO has set up a research centre in Tallinn, which is already open but will be formally inaugurated in 2009.

Mr Hollis points out that the debate about how best to classify cyberattacks has much in common with the debate about terrorism. Should terrorism be treated as a crime, as an act of war, as both at once, or as something entirely different that requires new laws? He favours this last approach for cyberattacks because it avoids the translation problems that arise when applying existing rules to such attacks, and because those rules are themselves somewhat outdated, given that attacks (in the real world and online) may come from non-state actors such as terrorist groups. Mr Hollis proposes a new “international law for information operations” to alleviate the uncertainty. He concedes that there is unlikely to be international consensus in this area soon, but argues that it would be a big step in the right direction if a group of states such as NATO, or the OECD club of industrialised nations, agreed to be bound by a clear set of rules.

What effect such co-operation would have on containing anonymous and unofficial cyberwarriors is hard to say; the fight against real-world terrorism does not offer much hope. And it is attacks from such groups that some researchers are most worried about. John Robb, a military futurist, calls the spontaneous, bottom-up mobilisation of volunteer cyberattackers in the Georgian conflict an example of “open-source cyberwarfare”.

This approach has several advantages over centralised, state-directed cyberattacks, he says. Leaving the attacks to informal cybergangs (the extent of the Russian state’s involvement remains unclear), rather than trying to organise a formal cyberarmy, is cheaper, for one thing. The most talented attackers, with the best tools, might not want to work for the state directly. Best of all, from the state’s point of view, is that it can deny responsibility for the attacks. It is the online equivalent of the use, by some governments, of gangs and militias to carry out attacks on political opponents or maintain control in particular regions.
Send in the botnet

There is no consensus among conventional military types about how to deal with such cyberattackers. Writing in *Armed Forces Journal* in May, Colonel Charles Williamson, of the intelligence and surveillance division of America’s air force, proposed that the United States should establish its own “botnet”—a network of machines “that can direct such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries than hunks of metal and plastic.” America, he wrote, “needs the ability to carpet-bomb in cyberspace to create the deterrent we lack.” The botnet could be built out of obsolete computers that would otherwise be discarded, he suggested. But he conceded that there would be legal and political difficulties associated with its use.

Mr Robb is sceptical of the ability of formal military organisations to wage cyberwarfare. “A few top people with the right tools can do the work of thousands of less capable people, so it’s better not to waste the money on 40,000 uniformed personnel dedicated to a bureaucratic and lethargic cyber command,” he says. And after an attack from an informal, self-organised group, there is no clear target to strike in any case. It may make more sense for existing military bodies to concentrate on defence, by identifying the most vulnerable parts and working out how to protect them. “Anything they can do to us, we should be able to counter faster—that’s the appropriate deterrence paradigm for this cyberage,” says Thomas Barnett, a military strategist at Enterra Solutions, a technology firm. “We should concentrate on making ourselves resilient.”

One way for governments to do this, says Richard Bejtlich, a former digital-security officer with the United States Air Force who now works at GE, an American conglomerate, might be to make greater use of open-source software, the underlying source code of which is available to anyone to inspect and improve. To those outside the field of computer security, and particularly to government types, the idea that such software can be more secure than code that is kept under lock and key can be difficult to accept. But from web-browsers to operating systems to encryption algorithms, the more people can scrutinise a piece of code, the more likely it is that its weak spots will be found and fixed. It may be that open-source defence is the best preparation for open-source attack.