The next war will be an information war, and we're not ready for it

November 27 2015, by

Aaron Ansarov

In the 21st century the familiar form of warfare in which physical damage is meted out against the opponent's military forces and infrastructure has become only one form of attack. Instead, states are increasingly launching non-lethal attacks against an enemy's information systems – this is the rise of information warfare.

Dan Kuehl of the National Defence University defined information

warfare as the "conflict or struggle between two or more groups in the information environment". You might say that just sounds like a fancier way of describing hacking. In fact it's a lot more sinister and a lot more dangerous than its somewhat tame name implies.

Western leaders are investing billions to develop capabilities matching those of China and Russia, establishing military commands for attacking, defending and exploiting the vulnerabilities of electronic communications networks. Information warfare combines electronic warfare, cyberwarfare and psy-ops (psychological operations) into a single fighting organisation, and this will be central to all warfare in the future.

The anatomy of information warfare

The free flow of information within and between nation states is essential to business, international relations and social cohesion, as much as information is essential to a military force's ability to fight. Communications today lean heavily on the internet, or via communications using various parts of the electromagnetic spectrum (such as radio or microwaves) through terrestrial communications networks or satellite networks in space. We live in a highly connected world, but it doesn't take much to tip over into instability or even chaos.

Electronic warfare is used to disrupt or neutralise these electromagnetic transmissions. These might be electronic counter measures and jamming used to cripple military communications or weapons guidance systems. Or it can include civil uses, for example the ADS-B air traffic control system used by aircraft to avoid in-flight collisions, or the recently adopted European Rail Traffic Management System (ERTMS) that replaces railway trackside signalling and provides full control of trains. Jamming or degrading either of these would cause chaos.

We have become familiar with cyber-attacks launched through the internet against digital networks, which can make it impossible for businesses to operate. Enormous damage can follow, in cost and reputation, as seen from attacks on Sony Pictures and TalkTalk. Bringing down a stock exchange could cause massive financial losses. Cyber-attacks can also be directed at industrial control systems used in manufacturing plants or in power, water and gas utilities. With the capacity to affect such a wide range of national infrastructure lives would be put at risk.

INFORMATION OPERATIONS INTEGRATION INTO JOINT OPERATIONS (NOTIONAL)

Core, Supporting, Related Information Activities	Activities	Audience/ Target	Objective	Information Quality	Primary Planning/ Integration Process	Who does it?
Electronic Warfare	Electronic Attack	Physical, Informational	Destroy, Disrupt, Delay	Usability	Joint Operation Planning and Execution System (JOPES)/ Targeting Process	Individuals, Governments, Militaries
	Electronic Protection	Physical	Protect the Use of Electro-magnetic Spectrum	Security	JOPES/Defense Planning	Individuals, Businesses, Governments, Militaries
	Electronic Warfare Support	Physical	Identify and Locate Threats	Usability	Joint Intelligence Preparation of the Battlespace(JIPB)/SIGINT Collection	Militaries
Computer Network Operations	Computer Network Attack	Physical, Informational	Destroy, Disrupt, Delay	Security	JIPB/JOPES/Targeting Process	Individuals, Governments, Militaries
	Computer Network Defense	Physical, Informational	Protect Computer Networks	Security	JOPES/J-6 Vulnerability Analysis	Individuals, Businesses, Governments, Militaries
	Computer Network Exploitation	Informational	Gain Information From and About Computers and Computer Networks	Security	JIPB/Targeting Process	Individuals, Governments, Militaries
Psychological Operations	Psychological Operations	Cognitive	Influence	Relevance	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
Military Deception	Military Deception	Cognitive	Mislead	Accuracy	JOPES/Joint Operation Planning	Militaries
Operations Security	Operations Security	Cognitive	Deny	Security	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
Supporting Capabilities	Information Assurance	Informational	Protect Information and Informatin Systems	Security	JOPES/J-6 Vulnerability Analysis	Businesses, Governments, Militaries
	Physical Security	Physical	Secure Information and Information Infrastructure	Usability	JOPES/Defense Planning	Businesses, Governments, Militaries
	Physical Attack	Physical	Destroy, Disrupt	Usability	JOPES/Joint Operation Planning	Governments, Militaries
	Counterintelligence	Cognitive	Mislead	Accuracy	JIPB/Human Intelligence Collection	Governments, Militaries
	Combat Camera	Physical	Inform/Document	Usability, Accuracy	JOPES/Joint Operation Planning	Governments, Militaries
Related Capabilities	Civil Military Operations	Cognitive	Influence	Accuracy	JOPES/Joint Operation Planning	Governments, Militaries
	Public Affairs	Cognitive	Inform	Accuracy	JOPES/Joint Operation Planning	Businesses, Governments, Militaries
	Public Diplomacy	Cognitive	Inform	Accuracy	Interagency Coordination	Governments

Figure I-3. Information Operations Integration into Joint Operations (Notional)

The joined-up approach to the many aspects of information warfare. Credit: US DoD

Psy-ops are aimed more at degrading the morale and well-being of a nation's citizens. This might include spreading false information, rumour and fear through social media and news outlets. The great level of connectedness that populations have today is a strength, but being instantly connected means that misinformation and fear can also spread rapidly, resulting in panic.

Information warfare, then, is the integration of electronic warfare, cyberwarfare and psychological operations, for both attack and defence.

Information war has already broken out

It's suspected that Russia has launched increasingly sophisticated non-lethal attacks on its neighbours, for example against Estonia, Georgia and Ukraine, which experienced an integrated onslaught of electronic, cyber-attacks and psychological operations.

There is convincing circumstantial evidence that the Baku-Tbilisi-Ceyhan gas pipeline in Georgia was targeted using a sophisticated computer virus which caused an uncontrolled pressure build-up that led to an explosion. Even the so-called Islamic State has shown it has a good understanding of how to use and manipulate social media for use in psychological warfare. IS is reportedly building greater cyberwar and electronic warfare capabilities, as it recognises that winning the information war is key.

A response to unconventional warfare

In response to the threat of information war the British Army has established two new formations: the 77th Brigade for dealing with psychological operations, and the 1st Intelligence, Surveillance and Reconnaissance Brigade which combines electronic warfare and

intelligence. Hundreds of computer experts will be recruited as reservists, trained with the help of GCHQ's Joint Cyber Unit.

These are moves in the right direction, but the approach is too piecemeal. A recent RAND Corporation report argued for a highly integrated approach to all aspects of information warfare in order to present an effective defence force. In the US, Admiral Michael S. Rogers released a Cyber Command vision statement, describing how it would defend Department of Defence networks, systems and information against cyber attacks and provide support to military and contingency operations. The US approach is more integrated but this is only the case within the military – from a national perspective both countries lack an overall integrated approach with a common command structure that includes threats to civilian infrastructure.

So while the concept of information war appears to be well understood the aspects of it are not being addressed together, and such siloed thinking could lead to gaps in our security. Western governments have failed to fully grasp the vulnerability of electronic communications and the enormous risks this poses to critical infrastructure, transport, and the safety of civilians.

The US director of intelligence has emphasised the enormity of the cyber-threat facing the US, while British General Sir Nicholas Houghton in a speech at Chatham House observed that most acts of physical war today incorporate an online aspect, where social networks are exploited to manipulate opinion and perception. He also acknowledged that the tactics employed by Russia combine aspects of information war and also counter-intelligence, espionage, economic warfare and the sponsoring of proxies.

We need to better understand the full scope of information warfare as it evolves, identify where we are most vulnerable, and then establish a

single point of responsibility to implement defence mechanisms. Because those adversaries that are unconstrained by western policies, or by ethical or legal codes, can and will exploit our vulnerabilities.

Source: The Conversation