Cyber war in Ukraine – business as usual for Russia

March 12 2014, by Bruce Baer Arnold

Credit: shlomp-a-plompa/Flickr, CC BY-ND

In a war – declared or otherwise – bravery and perseverance are not enough. Communications are important. Effectiveness means being able to command your troops and gather information. It also means being able to trust your communications. Disrupting and distorting

communications is a dark art, the "new black" in overt and covert conflict.

That's what we're seeing in Ukraine. Russia appears to be having a fine time covertly sabotaging Ukrainian networks.

Disrupting communications is a traditional strategy. Lincoln's horsemen stripped Jefferson's telegraph lines in raids early in the US Civil War. Churchill authorised cutting Atlantic cables to isolate the Kaiser the day after the UK declared war in 1914.

Since then the "black art" has flourished.

Lots of pros, very few cons

Cyberwar is attractive for a number of reasons:

- it doesn't result in easily identifiable bodies. No naked kids running from the napalm. No second-by-second computer game -style video as the drone hits a tank or (oops) rescuers
- it can be denied – there's no smoking gun and no formal declaration of hostilities – and it's just as much about suspicion as it is about substantive effect
- you can do much of it from the safety of your desk rather than while dodging bullets and listening to the screams of a dying compatriot
- it is a manifestation of modernity and prowess: the counterpart of the gatling guns, dreadnoughts and B52s that signalled "top nation".

In a networked and computer-dependent world it happens on both sides. In 2012, someone (Israelis, the US?) reportedly impeded the Iranian nuclear program through software dubbed "Flame" that sabotaged

equipment in Iran's enrichment facilities.

Russia appears to have engaged in undeclared disruption in Estonia, in Chechnya and in Georgia, such as preventing global access to Estonian government and news sites.

It appears to be doing the same in Ukraine and will, presumably, again deny any misbehaviour while simultaneously boasting about its capability.

So what's going to happen now?

Well, the answer is not clear.

Some Ukrainian telecommunications networks appear to be falling over: phone calls aren't getting through and Wi-Fi networks are sporadically unavailable. Distributed denial of service (DDoS) attacks mean that some official, business and civil society websites are unavailable.

Presumably others, including some hosted outside Ukraine, will soon go offline. Some will be hacked to feature obscenities or false information for people looking for news, reassurance, instructions. Ukrainian financial networks – pension payments, cross-border transactions, bank withdrawals – may be disrupted.

Such inconvenience and confusion is important in demoralising citizens, particularly officials. It is also important in inhibiting journalism and support from outside the targeted country, a stealthy digital addition to the conventional fog and noise of war.

Experience in Georgia and Estonia suggests that contrary to fears in the mass media we are not going to see planes dropping out of the sky over Kiev, dams collapsing, factories unexpectedly dumping toxic waste into

rivers, toasters or washing machines running amok and sewage plants being hijacked from a desktop in Moscow.

That is because in Ukraine most of that equipment is not networked or even computer-controlled.

As in Australia, operators can often rely on manual overrides and ingenuity. Experience in the Balkans over the past three decades demonstrates that people can cope without the internet, ATMs, television and even functional sewage systems – particularly if they are in good spirits.

Faith in cyberwar as a guaranteed knockout strategy may be as misplaced as past faith in the dreadnought, poison gas, the machine gun or bombing.

We should accordingly be wary about visions of a "cybergeddon", the digital apocalypse in which a frustrated Putin takes over your ATM or commandeers Bloomberg and the BBC. There will be the usual opportunism on the part of some Australian politicians and officials, with different agencies vying for more power and resources to deal with cyberthreats.

The Australian cyber-left – so outraged by legitimate intelligence activity on the part of the Australian Signals Directorate (ASD), so lamentably silent in critiquing NSA whistleblower Edward Snowden (whom we can assume to have shared his trove with Putin, deliberately or otherwise) – will fret reflexively.

The "West" has one effective response to Russian cyberwarfare in Ukraine. It is a digital response. Hobble the billions of assets that Putin and his associates in the "mafia state" have moved offshore. Hobbling would be bad news for the upper end of the London property market.

In a world of digits it would, though, be more persuasive than parking a gunboat near Crimea, scrambling North Atlantic Treaty Organisation's (NATO) fighters or hijacking the Kremlin's websites. Tether the bear with red tape.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Provided by The Conversation