The best time to wage cyberwar

Maths model calculates whether it is worth waiting to hit enemies at their most vulnerable.

Regina Nuzzo

13 January 2014

Peter Dazeley/The Image Bank/Getty Images

Malicious software can go off like a time-bomb but also has limited shelf life, as targets could discover and fix their code's security holes.

If you discover a way to hack into your enemy's computers, do you strike while the iron is hot, or patiently wait for a better opportunity to arise? Wait too long, and a vigilant enemy might spot its vulnerabilities and fix them. Strike too soon, however, and you will have blown your chance to wreak havoc when you might really need it.

A new mathematical model, built on analyses of double-agent spies and code-breaking during the Second World War[1], provides a way to calculate the ideal timing of a surprise cyberattack. The work, developed by political scientists Robert Axelrod and Rumen Iliev of the University of Michigan in Ann Arbor, is published this week in *Proceedings of the National Academy of Sciences*[2].

Modern cyberweapons can be sneaky. For example, when the Stuxnet computer worm infected an Iranian nuclear enrichment plant in 2009 and disabled many of its isotope-separation centrifuges, it managed to trick the control room so that the worm went unnoticed for almost a year and a half. The new model suggests that the better your malicious code is at burrowing undetected, “the more readily you can use it, because you won't have to worry as much about losing it — and you may be able to use it again”, Axelrod says. In this instance, unleashing Stuxnet as quickly as possible rather than waiting for a more opportune time was the 'rational' approach.

Sitting ducks

In conventional warfare, most situations are of small consequence (skirmishes without a great loss of life, for example). But a few situations have enormous stakes (large battles with thousands of casualties). If international cyberconflict were to follow the same pattern, then a rational nation should be patient and hold on to its cyberweaponry for those rare occasions when political stakes are high — just as Britain held off acting on information from its double agents until D Day was at hand, Axelrod says.

That does not mean that a country should feel safe when things are quiet: a rational opponent knows that stakes can change quickly and so is probably sitting on its best weapons until the right opportunity arises. Terrorists, by contrast, might want to cause as much damage as they can, and for them, “next month is not that different from this month”, says Axelrod. “They tend to use capabilities as soon as they get them.”

The shelf life of an unused weapon also plays a role in the rational timing of an attack. So-called zero-day cyberattacks rely on security vulnerabilities about which the target is blissfully unaware (thus giving the target “zero days” to prepare for the attack). If a group believes that the cyberweapon in its back pocket will not go obsolete any time soon — because its target is unlikely to patch important vulnerabilities on its own before a bug can sneak in — then it’s most reasonable to save the weapon for a high-stakes situation. Stuxnet, for example, probably had a short shelf life, Axelrod says, because it relied on four different computer vulnerabilities in the nuclear enrichment plant remaining open at the same time, so it was likely deployed as soon as possible.

Short-term gains

The findings therefore have the counter-intuitive implication that cybersecurity can hurt in the short term, something that is “absolutely fascinating”, says John Arquilla, a defence analyst at the Naval Postgraduate School in Monterey, California, who first coined the term cyberwar. If an opponent thinks your vulnerabilities will remain unfixed, they will assume their weapon to have a longer shelf life. “Whereas if we got really, really good at cybersecurity and decided to improve it, and we’re out there discovering vulnerabilities every day, we might actually spark a flurry of attacks upon ourselves,” he says.

Not all cyberexperts agree with Axelrod and Iliev's model. “This focus is too simplistic,” says political scientist Thomas Rid of King’s

College London, author of the book *Cyber War Will Not Take Place* (Hurst, 2013). “The more important policy question, as [a US presidential panel report] recognised last year, is whether using offensive resources is productive in the first place.” The model also ignores other valuable issues, he says, such as what happens when a cyberattack escalates a situation.

Axelrod admits that this model is a first step, and he hopes to expand it to include back-and-forth responses with an opponent, which would bring this work in line with his celebrated game-theory work on a problem known as the prisoner’s dilemma[3]. He points out that it took from 1945 until 1960 for analysts to develop a viable strategy of nuclear deterrence. “Our aspiration here is that it shouldn’t take 15 years to do the same thing with cyberconflict.”

Nature | doi:10.1038/nature.2014.14502

References

1. Axelrod, R. *World Politics* **31**, 228–246 (1979).
2. Axelrod, R. & Iliev, R. *Proc. Natl Acad. Sci. USA* http://dx.doi.org/10.1073/pnas.1322638111 (2014).
3. Axelrod, R. & Hamilton, W. D. *Science* **211**, 1390–1396 (1981).