End this phony cyberwar

Talk of combat in the fifth domain has become a fixture in Washington. But cyberwar has never happened and probably never will, says **Thomas Rid**

EXACTLY two decades ago, the RAND Corporation, an influential think tank, proclaimed that "cyberwar is coming!" In 2005, the US Air Force declared it would now "fly, fight, and win in cyberspace". The future of war would surely play out in that fifth domain, on top of land, sea, air and space. Dark warnings of "Cyber Pearl Harbor" soon became a staple of Washington discourse.

Leaks revealed last week that the US government spends a staggering $4.3 billion a year on cyber operations. In 2011, American intelligence agencies reportedly mounted 231 offensive operations. The US, it seems, is gearing up for cyber combat.

What would an act of cyberwar look like? History suggests three features. To count as an armed attack, a computer breach would need to be violent. If it can't hurt or kill, it can't be war. An act of cyberwar would also need to be instrumental. In a military confrontation, one party generally uses force to compel the other party to do something they would otherwise not do. Finally, it would need to be political, in the sense that one opponent says, "If you don't do X, we'll strike you." That's the gist of two centuries of strategic thought.

No past cyberattack meets these criteria. Very few meet even a single one. Never has a human been injured or hurt as an immediate consequence of a cyberattack. Never did a state coerce another state by cyberattack. Very rarely did state-sponsored offenders take credit for an attack. So if we're talking about war – the real thing, not a metaphor, as in the "war on drugs" – then cyberwar has never happened in the past, is not taking place at present, and seems unlikely in the future.

That is not to say that cyberattacks do not happen. In 2010, the US and Israel attacked Iran's nuclear enrichment programme with a computer worm called Stuxnet. A computer breach could cause an electricity blackout or interrupt a city's water supply, although that also has never happened. If that isn't war, what is it? Such attacks are better understood as either sabotage, espionage or subversion.

Code-borne sabotage is a real risk. Industrial control systems run all sorts of things that move fast and can burn: trains, gas pipelines, civilian aircraft, refineries, even elevators and medical devices. Many of these are highly susceptible to breaches, and information about system vulnerabilities is easily available.

Even so, the number of violent computer-sabotage attacks against Western targets is zero.

Why? Because causing havoc through weaponised code is harder than it looks. Target intelligence is needed. Control systems are often configured for specific tasks, limiting the possibility of generic attacks. Even if they happened, such attacks may not constitute a use of force.

"Cyberwar has not taken place in the past, is not taking place at present and is unlikely in the future"

The second threat is cyber espionage. Data breaches are not just a risk, but a real bleeding wound for the US, Europe and other advanced economies. But espionage is not war, and cyber espionage is not cyberwar.

Finally, there is subversion – using social media and other internet services to undermine established authority. It is not a surprise that subversives, from Anonymous and Occupy to Arab protesters, use new technologies. Twitter and Facebook have made organising non-violent protest easier than ever, often in the service of liberty and freedom. But again, subversion is not war, and cyber subversion is not cyberwar.

There are other problems with the concept of cyberwar. First, it is misleading. Closer examination of the facts reveals that what is happening is the opposite of war: computer breaches are less violent than old-style attacks. Violent sabotage is harder if it is done through computers, while non-violent sabotage is now easier and is happening more often: crashing websites, deleting files and so on. The same goes for espionage: infiltrating software and opening remote back doors is much less risky than sending in human agents and clandestinely bugging embassy walls.

Talk of cyberwar is also

disrespectful. Last year, the US Department of Defense considered creating a new Distinguished Warfare Medal for drone operators and developers of computer attacks. Real combat veterans protested vehemently when they learned that the award would have ranked higher than the Purple Heart. Secretary of Defense Chuck Hagel then scrapped the idea. Ending or saving the life of another human is an existential experience; deleting or modifying data is not.

Talk of cyberwar also kills nuance. Intelligence agencies have started to take "cyber" seriously. By doing so, signals-intelligence agencies such as the US National Security Agency and the UK's GCHQ, as well as human intelligence agencies, are updating their tradecraft for the 21st century. The West is beginning to have an overdue debate about what kind of intelligence activity is legitimate for a 21st century democracy, and where red lines should be drawn. Drawing these lines requires subtlety. It is time for this debate to drop the prefix "cyber" and call a spade a spade: espionage is espionage.

Finally, talk of cyberwar is in the interest of those with a harsher vision of the web's future. Many countries are tempted to take control of their "cyberspace". Authoritarian states like to tweak their technical infrastructure, their national laws and their firewalls to "protect sovereignty in cyberspace", as they like to say – which in practice means protecting intellectual property thieves from foreign pressure and rounding up dissidents at home.

The armed forces need to stay focused on fighting and winning the real wars of the future. That's hard enough. Let us not militarise the struggle for the free and liberal internet today. ■

Thomas Rid is a reader in the department of war studies at King's College London and the author of *Cyber War Will Not Take Place* (Hurst)

One minute with...

Andreas Raptopoulos

This entrepreneur believes that drone networks could be the roadways of the future in rural parts of the world

You think that drones could help get vital supplies to the one billion people without reliable access to roads?
That's correct. The key concept for us is a network of small drones. Alone, each of those vehicles could cover only a small segment of the transportation network, but together they can have a big spread.

Why not build roads?
Following the lead of road systems in the West is a nearly impossible task for the African continent. You're talking about a massive infrastructure investment and a huge ecological footprint. If you were to deliberately plan out an approach to transportation and logistics in Africa, would you do it in the same way? I'm convinced that the answer is no. Instead, I think you would use a few different modes of transportation – and one would be an aerial method like the drone network we're proposing.

Won't a drone network be expensive too?
For us, the most interesting thing happening with drones is in the super low cost category. The vehicles that you can buy today for $1000 can do amazing things, and it's just the beginning of this technology. Instead of big machines, like the ones the military use, we're thinking small.

So you're not thinking about mass transport of crops, but smaller items like medicines?
Initially, it will be for medicine and diagnostics – things that are lightweight, high value. But over time, as the technology matures, there's a clear opportunity to move heavier loads. That's the big dream of Matternet – to become a transportation method that will allow economic growth.

In your recent TED talk you said that drones could take HIV test samples from remote field clinics to a hospital. Tell us about this.
It's something we're trying to make happen. In Maseru, a district of Lesotho where we have done a case study, there are 47 clinics that collect blood samples and six labs that analyse them. First you put those on a map and see if there are reliable transportation links for any of them. Then, if not, you design a transport system using UAVs.

EMILY QUALEY/POPTECH

PROFILE
Andreas Raptopoulos is co-founder and CEO of Matternet, a company in Palo Alto, California, that is dedicated to using unmanned aerial vehicles (UAVs) for vital transport networks

You did some field trials last year in Haiti and the Dominican Republic. How did those go?
We took a few of our prototypes to see if they work well in hot and humid environments, and also to see how people felt about them and to explore some possibilities for how they could use the technology. I couldn't have been happier with the enthusiastic reception we got.

Cellphones have transformed life for many in Africa. Do you think the same could happen with drones?
Yes. It's a radical idea, but we believe that drones could do for transportation what mobiles did for communications. Fifteen years ago, if you had said that mobile telephones would give access to these extremely poor communities and enable their economic growth, nobody would have believed it. We believe it's the same for transportation.
Interview by Alison George