

35,176 views | Jul 18, 2013, 12:45pm

How Does Cyber Warfare Work?



Quora Contributor ⓘ
Consumer Tech

ⓘ This article is more than 2 years old.



What is cyber warfare?

Simply put, cyber warfare is the use of hacking to conduct attacks on a target's *strategic* or *tactical resources* for the purposes of *espionage* or *sabotage*.

That's neat, but we just used some more buzzwords here. Let's break it down even further:

- **Strategic or Tactical Resources:** This is a bit of military mumbo-jumbo that basically means "things that help countries express their political will and/or wage war." This can be a lot of stuff: guns, ammunition, and fuel for jets and

planes. It can also be less obvious stuff: the morale of the troops, the political will of the civilian public, and the economic well-being of the country as a whole.





If war was chess, tactical scale refers to moving each chess piece to capture other pieces. Strategic scale refers to how you actually win that game of chess vs. your opponent.

Today In: [Tech](#)



It's worth noting the difference between *strategic* and *tactical* scale. In military terms, tactical scale means stuff that's directly used in combat (lit: *focused on the ordered arrangement and [maneuver](#) of combat elements in relation to each other and to the enemy to achieve combat objectives*" - DoD Dictionary of Military and Assorted Terms).

Strategic scale is the scale higher than this: what it takes to win *wars* and not just single engagements and battles. This includes the resources at home necessary to supply and wage a war: supplies, guns, ammunition, factories, able-bodied men and women to man the lines, and a public willing to continue to fight.



Author of this post: Andy Manoske, Geeky VC

Remember the difference between tactical and strategic scale. This difference is *really* important later down the line when we answer the punchline question of **why does it threaten society**.

- **Espionage:** Espionage is basically taking information that wasn't meant for you. In the case of cyber warfare, you're going to be stealing tactical and strategic information: information about troop movements, the strengths and weaknesses of weapon systems, the dispositions of various and anything else about **sensitive** (read: necessary to wage war) resources that might be important to know.

- **Sabotage:** Also called "direct action," this is when we take an active role and go out there and do something. In cyber warfare sabotage can be something as benign as dropping a government's website to causing a nuclear meltdown at a nuclear plant. It's a pretty broad phrase, but just remember it means "do something" whereas espionage here means "learn something."

How does cyber warfare work?

Nation/State-sponsored hackers (hackers either in the military of a nation/state or supported by said state) attack computers and networks that are involved with sensitive resources within a country.

They do this like you would hack any other computer or system: you learn as much as you can about the system, you figure out its flaws, and you exploit those flaws to either gain control of that system or destroy it.



The PLAAF 5th generation J20 fighter compared to the USAF F-22 fighter. It is speculated that the J20's design benefited from classified research materials obtained through cyber espionage.

In the former case, you can then read privileged information not meant for you (espionage) that you could exploit to gain advantage over your adversary. You could learn how fast a missile flies and build a plane that can outrun it. You could learn where your target is moving troops and set up an ambush. You could learn about which scientists are important to developing those weapons, or which congressmen were instrumental in getting funding for said systems and personally attack them.

You can also sabotage people if you have control of those systems. What if I snuck a secret program into the source code of that missile that would allow me to remotely detonate it while it was on the ground? What if I could figure how the troops are communicating and gain access to their network so I could confuse them and sneak forces in to destroy them?

Worse, what if I attacked the civilian workers and politicians behind all of the above? I could defraud them by getting to their various system/network accounts and pretending I was them. Or I could use the information I gained to get leverage over them and force them to work for me (i.e.: blackmail them with info you found on their computer, kidnap their families with stuff you learned from their email, etc.).

Destroying these systems has a pretty obvious effect: you stop the computer control over the system and presumably stop it from functioning. A good example of cyberwarfare here is in using DDoS (Distributed Denial of Service Attacks) to shut down access to government websites and social media. This was an effective tactic used by the Russian during the South Ossetian War in 2008 to cause chaos and sow disinformation among the populace before and during Russia's invasion.

Who does it target?

Cyber warfare is going to target any sensitive industry in your opponent's infrastructure. This means obvious stuff like the military and defense and weapons manufacturers. It also means stuff like civilian factories that make weapons, mines, and other resource manufacturers that help those factories operate, and the national power grid that gives all of the above its necessary electricity.

In its scariest incarnation, cyber warfare could target the most important strategic asset a country has: its population. In this way, you could launch terrorist attacks meant to

destabilize or dishearten that population from fighting. This means doing scary things like hitting major financial sectors and causing economic damage to the country's economy (think about what things would be like if the NASDAQ unexpectedly shut down) and abruptly terminating public communication (think what would happen if the national cell networks all terminated and the internet went down).

Why does it threaten society?

I think cyber warfare is scary for two reasons:

1. **Strategic cyber warfare does not distinguish between civilians and military:** Just like nuclear weapons in the cold war, cyber weapons are just as likely to be targeting civilian resources as they are military ones. While a nuke is obviously way more damaging than a piece of malware is alone, a cyberattack can cause civilian casualties and deaths.

A great example of this is an attack on the national power grid. The national power grid is an obvious strategic resource for the US. If you took down the power grid through a cyber attack (something the US is rightfully concerned about), you would not just stop factories from building guns. You would also cause traffic accidents, interrupt surgeries, stop life-giving machines such as iron lungs, and basically just kill a whole mess of people across the country.

- **It's really hard to figure out who launched cyberattacks, and as such, governments don't have to be held accountable for their actions:** One area where cyberweapons are a lot worse than nuclear weapons is in attribution - figuring out who launched the weapon in the first place. It's really easy to hide where you're hacking a computer from because you can go through *proxies* that mask where your traffic is originally coming from. Even if you figured out where the computer came from, it's another huge problem to figure out who the person sitting behind the keyboard was - much less whether or not they were a government agent. Without attribution, you can't have accountability. And without accountability, stuff like deterrence and mutually assured destruction don't work. If a government isn't accountable for their cyber attacks during a cyber war, they could always go for the throat and launch damaging, quasi-

terrorist attacks like taking down a country's power grid or sabotaging industrial systems to physically (and dangerously) damage factories or cities. In both cases, innocent civilians are most likely going to die.

How much of it is government sponsored?

Great question. Honestly, nobody knows. There aren't numbers showing the bifurcation between hacking sponsored by countries vs. hacking sponsored by rogue states or movements like Al-Qaeda. This is one of the big problems with cyber warfare: it's asymmetrical in nature. A small country with a strong hacker elite can easily wound a huge country with a shoddy infrastructure but otherwise amazing military.

It's fair to assume that hackers supported by wealthy countries are certainly much more dangerous. Most first world countries are passably good at defending themselves from basic cyber attacks. Hackers supported by powerful countries are probably going to be more sophisticated, and can pull off attacks that circumvent such defenses and potentially can cause catastrophic civil and military damages.

This question [originally appeared on Quora](#). More questions on [Cyber Warfare](#):

- *[Is the US in a cyberwar with China, and we don't even know it?](#)*
- *[How is the data stolen by Chinese hackers used?](#)*
- *[How often do people attempt to hack into online bank accounts?](#)*



Quora: the place to gain and share knowledge, empowering people to learn from others and better understand the world.