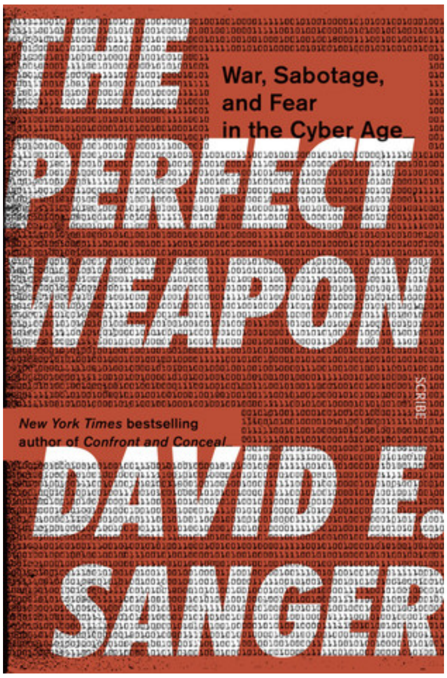
THE PERFECT WEAPON
War, Sabotage, and Fear in the Cyber Age
New York Times bestselling author of Confront and Conceal
DAVID E. SANGER
SCRIBE

The Perfect Weapon: How the Cyber Arms Race Set the World Afire

David E. Sanger

The Perfect Weapon: How the Cyber Arms Race Set the World Afire

David E. Sanger

The Perfect Weapon: How the Cyber Arms Race Set the World Afire David E. Sanger
From the premiere *New York Times* Washington correspondent, a stunning and incisive look into how cyberwarfare is influencing elections, threatening national security, and bringing us to the brink of global war.

Behind the Russian cyberattacks that may have thrown the 2016 election; behind the Sony hack; behind mysterious power outages around the world and the disappearance of thousands of personnel records from poorly guarded government servers are the traces of a new and powerful weapon, one that has the potential to remake global conflict like nothing since the invention of the atomic bomb. *The Perfect Weapon* is the riveting story of how, in less than a decade, cyberwarfare displaced terrorism and nuclear attacks as the greatest threat to American national security.

Cheap to acquire, difficult to defend against, and designed to shield their user's identities so as to complicate retaliation, these weapons are capable of an unprecedented range of offensive tactics; they can take us just short of war, allowing for everything from disruption to theft to the cause of widespread damage of essential infrastructure systems. And the vulnerability of those systems has created a related but equally urgent conflict: American companies like Apple and Cisco must claim allegiance to no government in the name of selling secure products around the globe yet the US intelligence agencies want the help of such companies in defending against future cyberattacks.

Reported and written with unprecedented access by *New York Times* chief Washington correspondent and bestselling author David Sanger, *The Perfect Weapon* takes readers inside war rooms and boardrooms, into the secret cyberdens of American and Chinese military, to give the deep-background story of the increasingly pitched battle between nations, their governments, their cyberwarriors, and their corporations.

The Perfect Weapon: How the Cyber Arms Race Set the World Afire Details

Date	:	Published June 19th 2018 by Crown
ISBN	:	9780451497895
Author	:	David E. Sanger
Format	:	Hardcover 384 pages
Genre	:	Nonfiction, Science, Technology, Politics, History

David E. Sanger

From Reader Review The Perfect Weapon: How the Cyber Arms Race Set the World Afire for online ebook

PrintedPagesandCoffee says

What David Sanger has produced here is a really excellent overview of the geopolitical, geostrategic implications of the increasing parties to cyber conflict and the capabilities to which they have access. Now, most of the book is about the implications of State use of cyber exploitation and attack capabilities or about States being victim to such and there are a lot of people who would argue that States aren't the be-all and end-all in cyberspace. Those people would be right, to an extent, but it is also the case that States are still the parties in cyberspace that have the legal monopoly over violence and, if pressed, have kinetic alternatives to cyber force in the event that cyber attacks fail to achieve the desired end. This means that States remain one of, if not the most important category of actor in the growing domain of cyber warfare, and they are likely to hold the position for some time yet.

The book itself is extremely well structured; the cases explored revolve around the United States of America as a matter of course (David is American and his specialty as a NYTimes reporter is security of/surrounding the U.S.) but give a thorough analysis of the perceived intent and goals of the opponents in each case. He also lays out, succinctly and coherently, the general threatscape with which States are currently trying deal as concerns cyberspace. There is no longer any actor in the international system today that is capable of laying constraints on cyber action: while the United States may once have enjoyed superiority in cyberspace that day is long past. States such as Russia, China, Iran and North Korea have ample capacity to utilize cyberspace as the threat and force multiplier that it is, and all of these States are also perfectly (and observably!) capable of employing cyberspace as an intelligence-rich domain. I have been saying for years, as have many scholars and experts, that cyberspace is an offensively-advantaged domain and that the opportunity cost of cyber attack is incredibly low relative to kinetic attack options. This hasn't changed. In fact, according to The Perfect Weapon, that is actually more evident today than it has ever been. General Nakasone, newly-minted head of NSA and Cyber Command, stated in his confirmation hearing that in cyberspace, the United States of America is not feared. This has serious implications for the attractiveness of the US as a target of malicious actors in cyberspace: they know that there will be little, if any, blowback for cyber attacks. Because there hasn't been previously: cyber defense is a lot more difficult, and more expensive, than cyber offense and that is evident in the volume and strength of cyber attacks that States endure every single day.

I found The Perfect Weapon to be incredibly well-written. The analysis of the cyber situation the US finds itself in was sound and, insofar as is possible within the length of a single book, both in-depth and detailed. I very much enjoyed reading it and look forward to anything else the David E. Sanger publishes in future. I can already so this book being useful in my own research and doctoral thesis.

Five star read, people!

Bruce Katz says

a serious and comprehensive look at cyber-warfare and the weaponization of social media: how they evolved, who the key actors are, the complicated legal and strategic questions surrounding them, the disputes among agencies, and much more. eye-opening, sobering, and even-handed in apportioning responsibility and, yes, blame. it deserves a wide readership... and a far more thoughtful review than i am capable of giving.

Scribe Publications says

In a chilling new book, The Perfect Weapon, *David Sanger details how more than 30 nations have developed effective cyber forces.*
Financial Times

[Sanger] writes with persuasiveness and authority.
The Telegraph

[Sanger is] a shrewd and insightful strategic thinker.
New York Times

An encyclopedic account of policy-relevant happenings in the cyberworld … the most comprehensive, readable source of information and insight about the policy quandaries that modern information technology and its destructive potential have spawned.
New York Times Book Review

Sanger, The New York Times*' security correspondent, has catalogued the recent history of how cyber warfare has developed, how it needs to be confronted, and the intensely complex policy issues that arise.*
Courier Mail

In his new book, The Perfect Weapon, *Sanger offers a panoramic view of the rapidly evolving world of cyber-conflict. He covers incidents from the covert U.S. cyber-campaign to sabotage Iran's nuclear program (a story we know about largely because of Sanger's diligent reporting) to Edward Snowden's epic heist of National Security Agency data. And yes, there's also plenty of background on Russia's active measures during the 2016 campaign. But there's also a wealth of gripping material on stories that have probably been missed by the broader public … It all adds up to a persuasive argument for the truth of the book's title.*
Christian Caryl, *The Washington Post*

*[*The Perfect Weapon *is] an important – and deeply sobering – new book about cyberwarfare.*
Nicholas Kristof, *New York Times*

Anyone who doubts cyber's unintended consequences should read David Sanger's new book The Perfect Weapon. *Sanger, a reporter for* The New York Times, *has been a dogged and diligent observer of cybersecurity issues for years. His book is a readable account of what went wrong.*
Robert Samuelson, *The Washington Post*

This encyclopedic account by a Times *correspondent traces the rapid rise of cyberwarfare capabilities and warns that ideas about how to control them are only beginning to emerge.*
***The New York Times Book Review* (Editor's Choice)**

Sanger, The New York Times' *security correspondent, has catalogued the recent history of cyber warfare, how it needs to be confronted and the intensely complex policy issues that arise. This is the last word in the modern world of cyber warfare – until artificial intelligence takes over.*

Mercury

Jacques Bezuidenhout says

Decent content and exciting (albeit scary) topic.
The narration on the audiobook however killed me from the inside a little. It was really a drag to listen to facts delivered in such a monotonous way.

I've done several other political books in the forms of The Dictator's Handbook: Why Bad Behavior is Almost Always Good Politics and Red Notice: A True Story of High Finance, Murder, and One Man's Fight for Justice. So the ways the governments operate and deceive isn't exactly new.

The cyber aspect is very interesting, though it doesn't really go into the nitty gritties.

There is a bit of an american feel/perspective to the book, which isn't really surprising considering the author works for the New York Times.

On the front of cyber crime/warfare I think no one is really prepared. And what the Americans think they know about what North Korea and the Russians are doing is probably only the tip of the iceberg.

Would only recommend if you are interested in politics and cyber warfare. And if you can get yourself to bare the narration. Reading might be better than listening with this one.

Mehrsa says

This is an excellent and terrifying read. The Russians and Chinese and North Koreans are in the house and it seems that this administration is not at all aware of the magnitude of the threat. Sanger has a lot of access and a depth of knowledge on the issues and this history. He's also an excellent writer. I do have some critiques--he seems to think that the olympic games project where the US and Israel hacked into the Iranian computer networks was completely justified (though he worries about its effects). I'm not so sure. Seems a bit sanctimonious to say--when we did it, it was totally responsible and justified. Now that everyone else is doing it, it's not.

D Schmüdde says

Sanger manages to cover the issue of cyberconflict broadly while also offering the most comprehensive account of what occurred during the 2016 election. He rarely infers, basing the accounts contained within on his sources from the top levels of the United States government.

Considering the role contractors play in the intelligence industrial complex, it would have been nice to have a greater representation of non-government sources, but the book never suffers from a lack of credibility.

It reads like a very long New York Times article with an op-ed at the end. This isn't necessarily I enjoyed, but I appreciate the author's pragmatism.

If you want to understand what's been happening at the dawn of information warfare, this is your book.

Mal Warwick says

Russia and China have penetrated so deeply into the electronic systems that sustain the American economy that either country might be able to set us back two or three decades using cyber weapons. North Korea and Iran appear to be not far behind. What seems to be stopping them all is the equal or greater ability of the United States to do the same or worse to them—not to mention the chance we might reduce their countries to cinders with nuclear weapons. That's the message at the heart of David E. Sanger's chilling new book, The Perfect Weapon. "Great power competition—not terrorism—is now the primary focus on US national security," he writes. And that competition is increasingly playing out online.

The US government has been slow on the uptake to acknowledge this threat. In 2007, the intelligence community's annual worldwide threat assessment delivered to Congress did not even include cyber weapons on the list. At that point, both Russia and China had been building their cyber capabilities for years. Now, of course, attitudes have changed. The United States Cyber Command, created in 2009, was upgraded only in 2018 into a Unified Combatant Command, one of ten in the US armed forces. Cyber Command is headquartered at Fort Meade, along with the National Security Agency, and is commanded by the agency's director. Together, NSA and Cyber Command house both our country's offensive and defensive cyber operations. Sanger explains that the two organizations work together uneasily. Their priorities are sometimes at cross-purposes.

Excessive caution about the threat of cyber weapons

David Sanger is extraordinarily well-connected in Washington. He has been writing on foreign policy, globalization, nuclear proliferation, and the presidency for more than thirty years for the New York Times. He has been the paper's Chief Washington Correspondent since 2006. Throughout The Perfect Weapon, he cites one-on-one conversations with nearly all the major players in the drama he describes. And drama it is. This book details the bureaucratic turf wars, foot-dragging, incompetence, and excessive caution that has so often characterized America's inadequate response to the threat posed by cyber weapons.

The dilemma Sanger describes is worrisome. "America's offensive cyber prowess has so outpaced our defense that officials hesitate to strike back," he writes. Although American companies and government are penetrated online thousands of times every day, the government has rarely spoken out to denounce those responsible. Partly, this is because it may take days, weeks, or even months to assemble definitive proof about who launched a given attack. But it's also because officials in the CIA, NSA, Pentagon, and White House are unwilling for our adversaries to gain any insight into how we obtained the information. Even when we know perfectly well who's responsible, they decline to speak out. Simply citing specific evidence could reveal the existence of American or Allied "implants" in their computer systems. Like many of the top former officials he interviewed, Sanger regards that reluctance to show our cards as an error.

"The US has only rarely activated cyber weapons"

Unless the government can accuse an adversary in public, it's hampered from retaliating. The upshot is that the US has only rarely activated cyber weapons, so far as we know. (The most notable exceptions were the Stuxnet attack on Iran's nuclear production facilities in 2010, carried out jointly with Israel, and the attack on North Korea's launch systems that caused its missiles to explode or fall into the sea.) However, Russia has not hesitated to attack weaker nations, chiefly Ukraine and Estonia, as well as both the United States and Western Europe.

As Sanger points out, there are ways, however inadequate, that the United States might combat a nuclear attack. There is always a warning, even if it's measured only in minutes. With cyber weapons, however, there is no warning. And "In almost every classified Pentagon scenario for how a future confrontation with Russia and China, even Iran and North Korea, might play out, the adversary's first strike against the United States would include a cyber barrage aimed at civilians." And the threat isn't limited to those four hostile countries. "A decade ago," Sanger notes, "there were three or four nations with effective cyber forces; now there are more than thirty." Now we face the proliferation of cyber weapons, not just nuclear devices.

About the author

David E. Sanger has written two books on American foreign policy as well as The Perfect Weapon, his most recent work. He is the Chief Washington Correspondent for the New York Times.

Alexander says

4.5 stars, rounding up. Sanger is one of the country's finest journalists on all issues cyber, and this book is frequently gripping and fascinating. It provides an in-depth look at a number of cyber incidents (including Olympic Games, which destroyed a number of the Iranian nuclear program's centrifuges).

But perhaps more importantly, Sanger pushes us hard to grapple with the need for an emerging framework of norms and laws around the use of cyberwarfare and warns (effectively, in my view) against the consequences of continuing down the path we have trod thus far.

Like many books adapted from reporting, it's unnecessarily repetitive in some places, while leaving some topics perhaps underexplored. Overall, though, the reporting is excellent, the topic crucial, and the thesis incredibly timely -- and it's a pretty easy read to boot.

ZaibatsuRandom says

Truth be told, for the most part this is an excellent book, with a great deal of good research. Unfortunately it is marred by a distinct political outlook that detracts from the fascinating story. The author is employed by the New York Times, so that should give an idea of how the book leans. There are so many good, solid parts in the book that when it slips into what can only be defined as partisanship it is so glaring. It's clear beyond any doubt that the author holds Donald Trump in complete disdain and is completely unwilling to utter a negative word about Hillary Clinton. So, large chunks of the story get left out and certain items are interwoven in a way that, even though they all happened before the Trump administration came into office, they seem much more incompetent than the previous administration.
I'd say, read the book with an open mind and a clear view of the underlying story the author is pushing. There are a couple places where he editorializes and his assertions have proven to be false, which also greatly detracts from the chapters that deal with the Trump campaign/presidency.
Legit Cave

Brandon Forsyth says

David Sanger is simply the best writer alive working on issues of global and American security, and his latest book proves how far ahead he is of everyone else in his field. His meticulous reporting and cogent analysis of where cyber warfare is headed makes an urgent argument for international standards (a "digital Geneva Convention" is mentioned) to be discussed and adopted with haste. From the Iranian centrifuge sabotage to Russian hacking of Ukrainian power systems and American election tampering, Sanger exposes how little-understood these new capabilities are, and makes a powerful case that this confusion could lead us to a very dangerous place. THE PERFECT WEAPON is a gripping, insightful read that I can't recommend enough.

Myles says

David Sanger's "The Perfect Weapon" is largely a compilation of reporting he and The New York Times produced over the past few years about American preparedness for cyberwarfare.

Sanger complains the America isn't prepared, has no policy or dividing line between cyberespionage and offensive attacks, has greater vulnerability than other nations because of its advanced economy, and is regularly giving up secrets because of the porousness of its government's own networks.

Really there's little new here.

In spite of the lessons learned from the 9/11 attacks, it sounds as though the American intelligence community is once again at war with American offensive capability: the spooks fear sharing their knowledge of their foes with the defence establishment who want to intrude and cripple the enemy.

And the enemy is getting smarter. In addition to stealing American secrets, Chinese investment is buying into Silicon Valley startups and getting full warning about what is on the horizon.

What anyone will find alarming about this analysis is that few in Washington know when or if to use conventional weapons in this new environment.

The current confusion over Russian meddling in the 2016 election being a case in point. Donald Trump aside, America is unsure what the most useful response to Putin should be, what will be a sufficient disincentive to future meddling both in American infrastructure and those of its allies. (NOTE: As I write this Chinese countervailing duties target Republican strongholds in the MidWest. Why Russian trolls count as "political meddling" in internal US affairs and the Chinese blowback doesn't escapes me.)

This is what Trump ought to be hashing out at NATO meetings.

If the Stuxnet attacks on Iranian centrifuges showed American and Israeli cyberforces on the forefront, much of that lead may have disappeared as Russia, China, Iran, and North Korea throw greater and greater resources at the problem.

Korea has even resorted to cybercrime to finance their programs.

But these vulnerabilities raise an even more fundamental issue: think back to the invention of the Internet by contractors working for DARPA. The original purpose of the Internet was to distribute control of American defence command to withstand a debilitating nuclear attack.

It is the very structure of the Internet which is opening American vulnerabilities, giving safe haven to America’s foes, and is proving a fertile testing ground for new and diabolical weapons of mass destruction.

Here again technology is coming back on itself. America’s (and our) foes are throwing its weapons back at itself very, very quickly. When it took years for the Soviets to replicate the American Atomic bombs and delivery mechanism, and its hydrogen bombs, the timeline for stealing NSA weapons and throwing back against the allies has dramatically shrunken.

This has the potential to dramatically increase tensions and destabilize all of our societies.

Overlay these tensions with advances in AI, genetic engineering, climate change, and new techniques to 3D print and distribute weapons, and you get one heck of a toxic environment.

That really sucks.

Chris says

A fascinating portrait of the rise of hybrid warfare against the United States that devastatingly illustrates how American national security leaders' obsessive secrecy and paralyzing caution ultimately enabled a gallery of rogue nations to outmaneuver them, culminating in the inept response to the Russian hacks of the 2016 election.

Gamespacenl says

Very well written, timely, informative, no-frills account of cyber weaponry and warfare from a decidedly US perspective.

---

itpdx says

As the author says this is just what is known. From the cyber attack on Iran’s nuclear enrichment facility to election interference to North Korea’s bank heist, Sanger puts together a report of what is publicly known (more or less) of the current cyber war. He lets us in the on the policy debates— is the US government responsible for defending or countering an attack on a global company, should the US government require back doors into encryption, should Defense take an action that would tip-off opposing governments to our spy capabilities?

This is the book that puts together the headlines and news stories of the last decade and in perspective. And asks the questions that the world needs to debate.

Radiantflux says

66th book for 2018.

Nice summary of current situation around cyberwar from an American perspective. This is a scary world where large state players (China and Russia, but also North Korea and Iran) are increasingly intruding (attacking?) US targets. The US is largely unprotected from a cyberattack, which could take down power, water etc. relatively easily. Having read this it's really unclear how secure US voting systems are from an attack during 2018 election cycle.

Well worth a read. A nice complement to Russian Roulette which covers some of the same material as it relates to Russia's hacking of the 2016 US Elections.

4-stars.