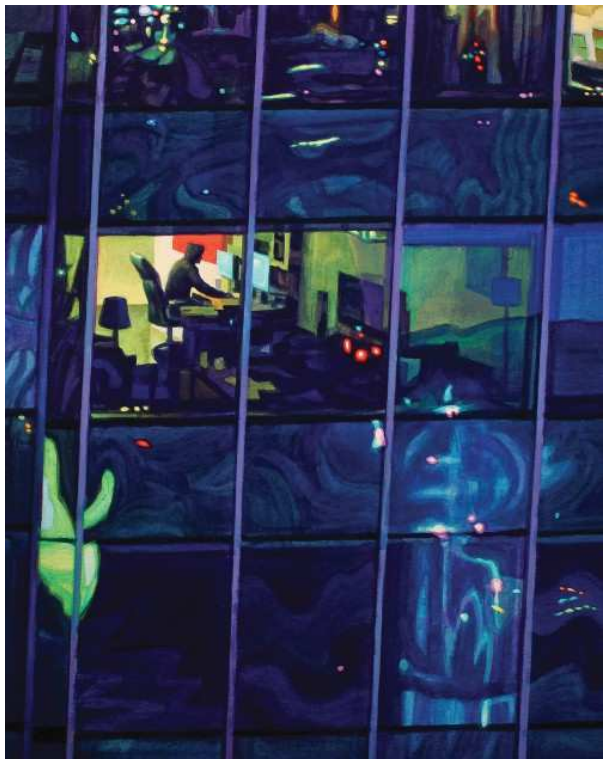
Business

Mr. Robot Killed the Hollywood Hacker



The popular portrayal of computers as magic boxes capable of anything has done real societal harm. Now one TV show wants to save us.

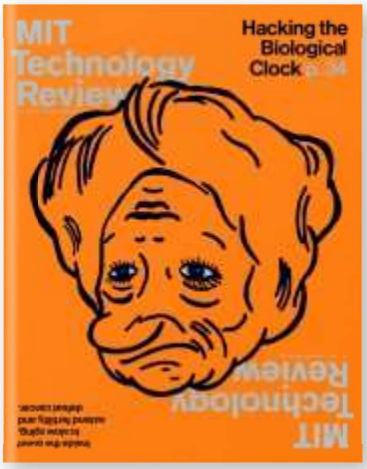
by Cory Doctorow December 7, 2016

For decades Hollywood has treated computers as magic boxes from which endless plot points could be conjured, in denial of all common sense. TV and movies depicted data centers accessible only through undersea intake valves, cryptography that can be cracked through a universal key, and e-mails whose text arrives one letter at a time, all in caps. "Hollywood hacker bullshit," as a character named Romero says in an early episode of *Mr. Robot,* now in its second season on the USA Network. "I've been in this game 27 years. Not once have I come across an animated singing virus."

Mr. Robot marks a turning point for how computers and hackers are depicted in popular culture, and it's happening not a moment too soon. Our thick-headedness about computers has had serious ramifications that we've been dealing with for decades.

Following a time line of events from about a year before the air date of each episode, *Mr. Robot* references real-world hacks, leaks, and information security disasters of recent history. When hackers hack in *Mr. Robot*, they talk about it in ways that actual hackers talk about

hacking. This kind of dialogue should never have been hard to produce: hacker presentations from Black Hat and Def Con are a click away on YouTube. But *Mr. Robot* marks the first time a major media company has bothered to make verisimilitude in hacker-speak a priority.



This story is part of our January/February 2017 Issue

See the rest of the issue

Subscribe

Mr. Robot: Season 1, Episode 3 - (Spoiler) 'Elliot Hacks His H...

The show excels not only at talk but also at action. The actual act of hacking is intrinsically boring: it's like watching a check-in clerk fix your airline reservation. Someone types a bunch of obscure strings into a terminal, frowns and shakes his head, types more, frowns again, types again, and then smiles. On the screen, a slightly different menu prompt represents the victory condition. But the show nails the *anthropology*

of hacking, which is fascinating as all get-out. The way hackers decide what they're going to do, and how they're going to do it, is unprecedented in social history, because they make up an underground movement that, unlike every other underground in the past, has excellent, continuous, global communications. They also have intense power struggles, technical and tactical debates, and ethical conundrums—the kind of things found in any typical *Mr. Robot* episode.

Things reviewed

Mr. Robot
USA Network

Black Mirror
Britain's Channel 4

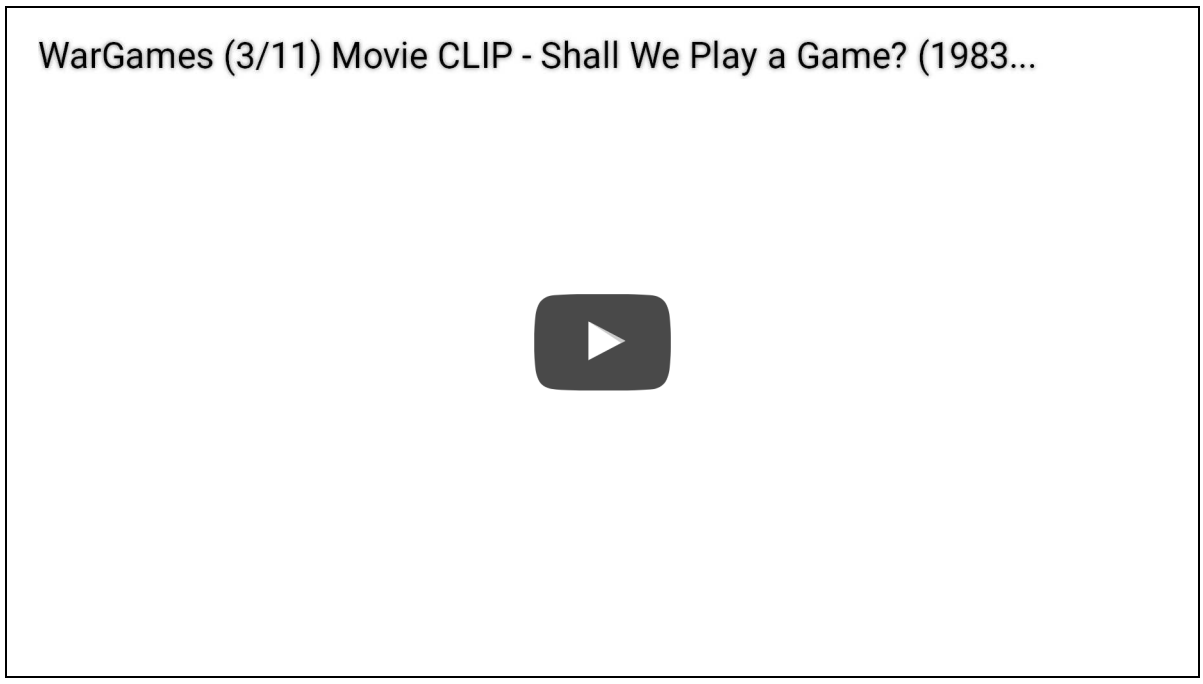
The Computer Fraud and Abuse Act

Mr. Robot wasn't the first technically realistic script ever pitched, but it had good timing. In 2014, as the USA Network was deliberating over whether to greenlight *Mr. Robot*'s pilot for a full season, Sony Pictures Entertainment was spectacularly hacked. Intruders dumped everything—prerelease films, private e-mails, sensitive financial documents—onto the Web, spawning lawsuits, humiliation, and acrimony that persists to this day. The Sony hack put the studio execs in a receptive frame of mind, says Kor Adana, a computer scientist turned screenwriter who is a writer and technology producer on the series. Adana told me the Sony hack created a moment in which the things people actually do with computers seemed to have quite enough drama to be worthy of treating them with dead-on accuracy.

It's about time. The persistence until now of what the geeks call "Hollywood OS," in which computers do impossible things just to make the plot go, hasn't just resulted in bad movies. It's confused people about what computers can and can't do. It's made us afraid of the wrong things. It's led lawmakers to create a terrible law that's done tangible harm.

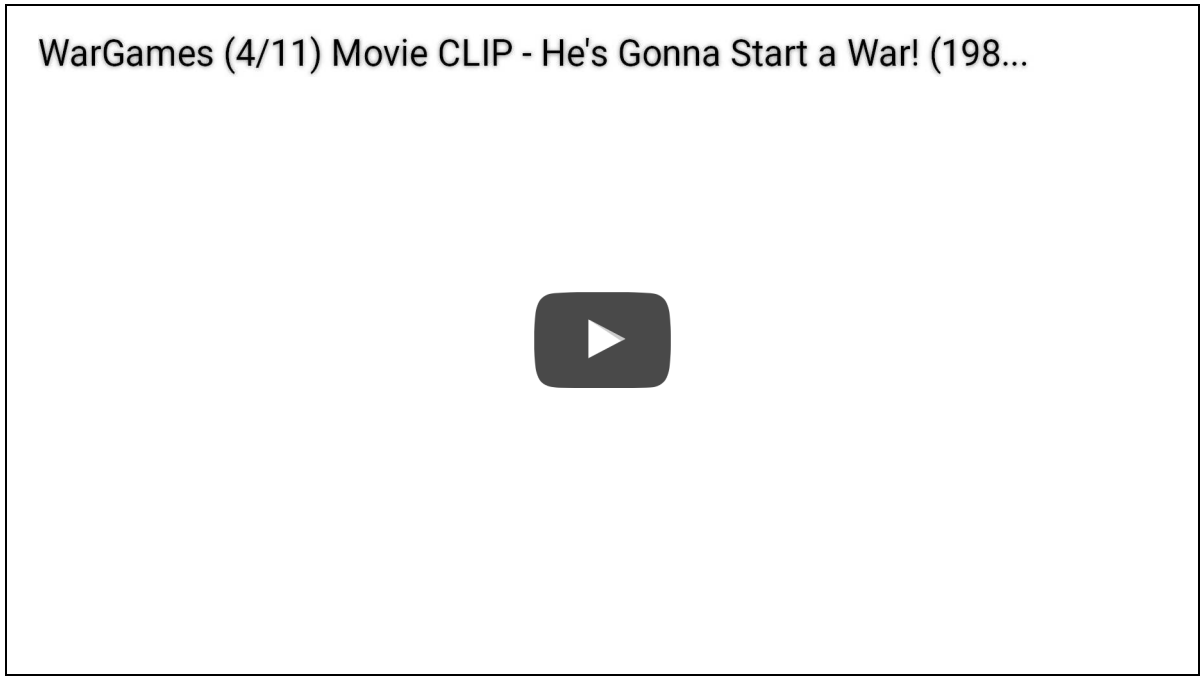
Worst law in technology

In 1983, Matthew Broderick had his breakout role as David Lightman, the smart, bored Seattle teen who entertains himself in *WarGames* by autodialing phone numbers with his computer's primitive modem, looking for systems to hack into and explore. When he connects to a mysterious system—seemingly an internal network for a game development company—he nearly starts World War III, because that "game company" is actually the Pentagon, and the "Global Thermonuclear War" game he's initiated is the autonomous nuclear retaliatory capability designed to launch thousands of ICBMs at the USSR.



WarGames inspired many a youngster to scrounge a 300-baud modem and experiment with networked communications. Linguistically, it gave us "wardialing" (dialing many phone numbers in sequence), which begat "warwalking" and "wardriving" (hunting for open Wi-Fi networks). The film wasn't a terrible approximation of how a misfit kid might have tried to hack in, although *WarGames* did make it seem as if the system had fewer fail-safes than it actually did. (Still, it also appears to be true that in real life the launch code for all the missiles was set to

"00000000.")



The worst thing about *WarGames*—and its most profound legacy—was the reaction of panicked lawmakers.

Passed by Congress in 1984 and broadened in 1986, the Computer Fraud and Abuse Act was a sweeping anti-hacking bill inspired by the idea that America's Matthew Brodericks could set off Armageddon. Before CFAA's passage, prosecutions against hackers had invoked a hodgepodge of legal theories. Crooks who broke into sensitive databases were charged with theft of the electricity consumed in the transaction.

CFAA's authors understood that even if they explicitly banned the hacking techniques of the time, these prohibitions would swiftly be overtaken by advances in technology, leaving future prosecutors scrounging for legal theories again. So CFAA took an exceptionally broad view of what constitutes criminal "hacking," making a potential felon out of anyone who acquires unauthorized access to a computer system.

It sounds simple: you can legally use a computer only in ways its owner

has permitted. But CFAA has proved to be a pernicious menace—what legal scholar Tim Wu has called "the worst law in technology." That's because companies (and federal prosecutors) have taken the view that your "authorization" to use an online service is defined by its end-user license agreement—the thousands of words of legalese that no one ever reads—and that violating those terms is therefore a felony.

This is how a young entrepreneur and activist named Aaron Swartz came to be charged with 13 felonies after using a script to automate his downloads of articles from JSTOR, a scholarly repository on MIT's networks. Swartz was legally permitted to download these articles, but the terms of service forbade using a script to fetch them in bulk. What Swartz did was no accident—he made multiple attempts to get around JSTOR's download limits over a period of months, and ultimately entered a basement wiring closet to tap into a network switch directly. But because of CFAA he was facing up to 35 years in prison when he hanged himself in 2013.

Decades ago, WarGames inspired a legacy of stupid technology law that we still struggle with. Mr. Robot might just leave behind a happier legacy.

After *WarGames*, Hollywood made a trickle of "hacker movies," many much beloved by actual hackers. There was 1992's *Sneakers*, which took some of its inspiration from real-world phone phreaks John "Cap'n Crunch" Draper and Josef "Joybubbles" Engressia. There was 1995's *Hackers*, which referenced the 2600: Hacker Quarterly meetups and Operation Sundevil, the Secret Service's notorious 1990 hacker raids (which resulted in the founding of the Electronic Frontier Foundation).

But even these movies wanted for much in the way of technical accuracy. *Sneakers* ridiculously featured a universal key that can break

all crypto; *Hackers* featured the graphically elaborate virus mocked by Romero in *Mr. Robot*. The films featured the kinds of musical viruses and absurd user interfaces that are the desperate hallmarks of a visual medium trying to make a nonvisual story interesting.

It only got worse. As cryptography crept into the public eye—first through the mid-1990s debate over the Clipper Chip, which would have put a backdoor in essentially all computers, then through subsequent political fights that rage on to this day—it became a frequent source of plot points and groans of dismay from actual hackers and security experts. Like the moment in the fifth *Mission Impossible* movie when hackers replace the contents of an encrypted file with 0s without first decrypting the file, or the way in *Skyfall* that encrypted data is visualized as a giant moving sphere. Crypto in movies works just like crypto in the minds of lawmakers: perfectly, until it needs to fail catastrophically.

Rami Malek plays Elliot on Mr. Robot, a show that marks the first time a studio has bothered to prioritize accuracy in how it portrays hacker culture.

Fan noise

Kor Adana is largely responsible for giving *Mr. Robot* the technological rigor that sets the show apart. The 32-year-old Michigan native once worked at an automotive company, attempting to punch holes in the security of the computers in cars heading into production.

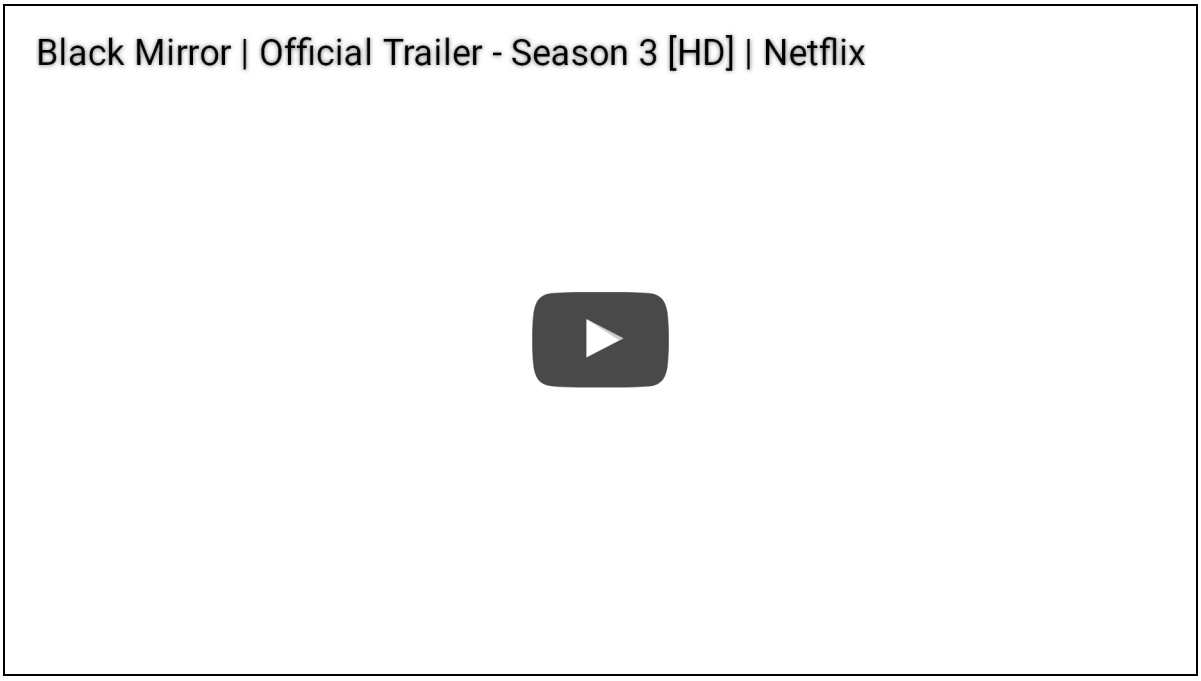
READER COMMENT View All

Along the same vein, TV shows of forensic science where, for example, full DNA analysis is done in under an hour. And all results are 100% correct.

– yu tube

Adana told me that when he threw away his lucrative cybersecurity career to work in Hollywood, he was gambling that his background in information security would be an asset rather than an odd quirk. That paid off thanks to the trust of show creator Sam Esmail, who gave Adana the authority to argue with production designers over seemingly minor details. He ensures that the correct cable connects a PC tower to its monitor, or that the network card's activity lights are actually blinking when the shot comes out of post-production. Adana gives sound engineers fits by insisting that scenes set in rooms full of powerful PCs must have the correct level of accompanying fan noise.

Adana also battles the legal department over his commitment to technical rigor in the hacking attacks depicted on the show, knowing that hackers will go through the episode frame by frame, looking at the command-line instructions for accuracy and in-jokes. Those hackers are a minority of the show's audience, but they're also the show's cheerleaders, and when an incredulous information civilian asks a clued-in hacker buddy whether the stuff on *Mr. Robot* could *really* happen, the hacker can nod vigorously and promise that it's all true.



Another promising show is *Black Mirror*, created by the British satirist Charlie Brooker and now streaming on Netflix. It's not rigorous in the same way as *Mr. Robot*, because it projects into the future rather than describing the technical details of the recent past. But its depiction of user interface elements and product design reflect a coherent understanding of how the technologies of today work, and thus where they may be tomorrow. Clicks on computers in the show call forth menus that have options we can recognize; the opacity of the error messages is all too plausible; even the vacant facial expressions of people lost in their technology have a plausibility that other shows rarely achieve.

My own 2008 young adult novel *Little Brother*, whose plot turns on the real capabilities of computers, has been under development at Paramount for a year now. The story features a teenage hacker army that uses GPS to send private e-mails and exploits software-defined radios in game consoles to create mesh networks protected by strong crypto. The one thing everyone in the meetings agrees on is that the technical rigor of the story needs to be carried over onto the screen.

This isn't trivial. It's not just about better entertainment. When information security is the difference between a working hospital and

one that has to be shut down (as was the case with the ransomware attacks on hospitals across America in 2016) and when server break-ins can affect the outcomes of U.S. elections, it's clear that we all need a better sense of what computers can do for us and how they can burn us. Adana says he is gratified when he meets information security noncombatants who have no interest in being IT nerds but who *are* interested in the security and privacy implications of the technologies they use—something heretofore believed to be impossible.

As cryptography crept into the public eye, it became a frequent source of plot points and groans of dismay from actual hackers and security experts.

Information security is one of those problems whose very nature can't be agreed upon—and the lack of technological smarts in the halls of power is compounded by the lack of technological understanding in the body politic. Decades ago, *WarGames* inspired a legacy of stupid technology law that we still struggle with. *Mr. Robot* and the programs that come after it might just leave behind a happier legacy: laws, policies, and understanding that help us solve the most urgent problems of our age.

Cory Doctorow is a science fiction novelist; his next book, Walkaway, *will be published in 2017. He is also a special advisor to the Electronic Frontier Foundation and activist in residence for the MIT Media Lab.*