

JOSH SCHULTE SENTENCED TO 40 YEARS

Aldrich Ames was arrested at the age of 53 in 1994 after 9 years of spying for Russia. He remains imprisoned in Terre Haute to this day – 30 years and counting – at the age of 82. (My math here is all rough.)

Robert Hanssen was arrested in 2001 at the age of 57 after 22 years of spying for Russia. He died last year, at the age of 79, in Florence SuperMax.

After six years in jail – most under Special Administrative Measures sharply limiting his communication – Josh Schulte, aged 35, was sentenced Thursday to 40 years in prison. He will presumably go to either Florence (most likely, because Judge Jesse Furman recommended he should go to someplace close to Lubbock) or Terre Haute.

Since his guidelines sentencing range was life in prison, I'm not sure how much, if any, of his sentence could, hypothetically, be dropped for good behavior.

Furman sentenced him concurrently on his Child Sexual Abuse Material conviction and the Espionage Act charges. Barring any successful appeal, he would be in prison for at least 20 years on top of time served, if he were to get credit for good behavior. That would put him back on the street at age 55, still the prime of his life (says someone in precisely that prime of her life, someone still learning some of the forensic techniques Schulte mastered as a teenager).

But the possibility that Schulte would be released before 2058, when Schulte will be 69, is based on two very big assumptions (on top of my uncertainty about whether he could get time off). First, that Schulte could sustain "good

behavior” in prison, when he has failed to do so even while being held under SAMs in New York. Most recently, the government alleges he somehow obtained *more* CSAM in 2022 while in prison, where he would consume it in his cell after days representing himself in his second trial, the one in which he was convicted of the Espionage Act charges.

Even while Schulte’s family was traveling to attend his trial in 2022, he chose to retreat to his cell to view the child pornography that he had secreted on his prison laptop. (See D.E. 1093-1 at 3-4 (describing examples of times when videos were played).)

And there’s good reason to believe he attempted to – may well have succeeded at – conducting further hacks from prison.

That’s some of what I’ve been pondering since the government first requested that Schulte be treated like four men, including Ames and Hanssen, who gave America’s secrets *to Russia* rather than giving them *to WikiLeaks*, as a jury convicted Schulte of doing, by sentencing him to life in prison.

It took years of tradecraft to recruit and cultivate sources like Ames and Hanssen.

Many of the details about what led up to Schulte’s leaks of the CIA’s hacking tools remain unknown – including via what server he shared the files, because WikiLeaks’ submission system could not have accepted them at the time, meaning Schulte *necessarily* had some kind of contact with WikiLeaks in advance.

But the current story is that Schulte reacted to being disciplined at work fairly directly by stealing and then sharing the CIA hacking tools in one fell swoop. In a matter of days in April and May 2016 (perhaps not coincidentally, the same period when Russian hackers were stealing files from Hillary Clinton’s team), Schulte took steps that burned a significant part of CIA’s

capabilities to the ground.

As a result of that reactive decision, Schulte delivered a set of files that would allow their recipients to hunt down CIA's human sources based off the digital tracks they left in highly inaccessible computers. As I've noted, Schulte was well aware of the damage that could do, because he wrote it up in a self-serving narrative after the fact.

I told them the confluence server was the one that seemed to be compromised, and while horrible and damaging at least it wasn't Stash; At least not at this point—Hopefully they could stop any additional leaks from the network at this point. From the news articles I've read, wikileaks claims to have source code, but we don't know what code or from where. However, at this point, I knew the SOP was a complete stand down on all [redacted] operations. We had no idea what had been leaked, when, for how long, or even who else had seen the materials leaked. Have they been steadily accessing our network every day? Have all our ops been blown since we wrote the first line of code? Perhaps only confluence had been leaked, but the individual(s) responsible are/were planning to exfil the other parts of DEVLAN too? So much still unknown, and with potential (yet unconfirmed) link between wikileaks and Russia—**Did the Russians have all the tools?** How long? It seems very unlikely that an intelligence service would ever leak a nation's "cyber weapons" as the media calls them. **These tools are MUCH more valuable undiscovered by the media or the nation that lost them.** Now, you can secretly trace and discover every operation that nation is conducting. I told them all this was certainly very disturbing and I felt bad for my friends and colleagues at the agency who likely

weren't doing anything and most likely
had to completely re-write everything.
[my emphasis]

What gets virtually no coverage is that this is precisely what happened: the bulk of the most sensitive files Schulte stole, the source code, has never been publicly accounted for. That's why I find credible the unsealed and sealed filings submitted with sentencing claiming that Schulte caused what Judge Furman claimed (as reported by Inner City Press) was \$300 million in damage and a cascading series of compromises.

Because DOJ couldn't trade a death sentence in exchange for cooperation about how Schulte did it, as they did with Ames and Hanssen, because digital encryption is much more secure than a dead drop in a Virginia park, it's not clear whether the government even knows all of it.

I don't even know what Schulte was trying when he attempted to social engineer me from jail in 2018 – but I have my suspicions.

Later this month, Julian Assange will get a last chance to stave off extradition. I have long suspected if the UK approves the extradition, Russia will attempt to swap Evan Gershkovich for Assange. One way or another, we may learn more about what the US government has learned about the WikiLeaks operation in the 7 years since Schulte was part of one of the most successful, sustained attacks by Russia on the US.

But until then, Schulte will be moving to new long-term accommodations in a highly secure prison.