# CIA’s fake Star Wars fan site exposed deep operational security failures that endangered spies



The Central Intelligence Agency (CIA) has revealed a remarkable aspect of its operational history: the use of fake websites, including a Star Wars fan site, to communicate with spies stationed around the globe. This revelation, uncovered by amateur security researcher Ciro Santilli, sheds light on a misguided communication strategy employed by the agency in the early 2000s, which ultimately had dire consequences for its informants.

Among the various fictional sites Santilli tracked down was StarWarsWeb.net, adorned with nostalgic imagery, including a boy dressed as a Jedi and beloved droids like R2-D2 and C-3PO. Such seemingly innocuous web pages, laden with advertisements for retro video games and LEGO sets, had a darker purpose: they served as covert communication channels for CIA operatives. Various other fan sites dedicated to comedian Johnny Carson, extreme sports, and Brazilian music were also part of this network, each tailored to specific geographical targets, including France, Spain, and Brazil, which were selected based on language and content relevance.

The covert communication system functioned discreetly; spies needed only to enter a password into the site's search bar, triggering a hidden messaging window to connect with their handlers. However, this strategy was fundamentally flawed. In a scathing assessment of the operational security, Bill Marczak from the University of Toledo's Citizen Lab said the system "stuck out like a sore thumb." The subsequent discovery of these sites by foreign intelligence agencies, particularly in Iran and China, contributed to the exposure and termination of numerous CIA operatives.

The agency faced significant backlash in 2011 and 2012, when Iranian and Chinese authorities dismantled several CIA networks and executed or imprisoned many informants. Although the CIA only learned of these compromised channels by 2013—when agents began to mysteriously vanish—an earlier report has indicated that the vulnerabilities were so prominent that even amateur investigators could have easily unearthed them. The mishandling of these digital communications points not only to operational flaws but also to strategic miscalculations regarding foreign intelligence capabilities.

In a troubling twist, the CIA knew about the security inadequacies of these mass-produced sites. They were primarily used for informants who were not fully vetted or were deemed to have limited access to sensitive information. Meanwhile, higher-tier informants were equipped with more advanced, customised communication tools. Yet, the widespread use of poorly constructed websites represented a significant lapse in security discipline. The fallout from this incident led to closed-door hearings in Congress and a comprehensive internal review by the CIA. In a 2021 memo, the agency acknowledged its "communications failure," reprimanding operatives for their lax tradecraft and overzealous pursuit of intelligence at the expense of security.

Reflecting on the findings, Santilli expressed a dual motivation for his investigation: a keen interest in geopolitical dynamics and a desire to expose the CIA's surveillance practices within democratic nations. He noted that the range of websites uncovered underscores not only the agency's operational interests but also a disturbing prioritisation of intelligence over the safety of human assets. The implications are grave; the unmasking of CIA operations may shake the foundations of trust essential for affiliations that intelligence agencies rely upon in sensitive environments.

Zach Edwards, another independent cybersecurity expert, remarked on the broader significance of these findings, indicating that even in the realm of perhaps the most secure operations, developers can commit errors leading to catastrophic consequences. The nature of espionage and intelligence gathering continues to evolve, but this particular episode serves as a cautionary tale about the interplay between technology and security—emphasising the need for relentless vigilance and sophisticated tradecraft in an increasingly interconnected world.

## Reference Map:

* Paragraph 1 – [[1]](https://www.dailymail.co.uk/news/article-14752155/CIA-fake-websites-Star-Wars-communicate-spies.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[4]](https://gizmodo.com/cia-websites-reportedly-led-to-the-exposure-of-critical-1849601326)
* Paragraph 2 – [[1]](https://www.dailymail.co.uk/news/article-14752155/CIA-fake-websites-Star-Wars-communicate-spies.html?ns_mchannel=rss&ns_campaign=1490&ito=1490), [[2]](https://www.theguardian.com/us-news/2022/sep/29/cia-websites-security-sources-communication-safety)
* Paragraph 3 – [[3]](https://www.overtdefense.com/2022/10/05/poorly-designed-cia-websites-likely-got-spies-killed/), [[6]](https://www.overtdefense.com/2022/10/05/poorly-designed-cia-websites-likely-got-spies-killed/)
* Paragraph 4 – [[2]](https://www.theguardian.com/us-news/2022/sep/29/cia-websites-security-sources-communication-safety), [[5]](https://www.theguardian.com/us-news/2022/sep/29/cia-websites-security-sources-communication-safety)
* Paragraph 5 – [[4]](https://gizmodo.com/cia-websites-reportedly-led-to-the-exposure-of-critical-1849601326), [[6]](https://www.overtdefense.com/2022/10/05/poorly-designed-cia-websites-likely-got-spies-killed/)
* Paragraph 6 – [[7]](https://gizmodo.com/cia-websites-reportedly-led-to-the-exposure-of-critical-1849601326)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.dailymail.co.uk/news/article-14752155/CIA-fake-websites-Star-Wars-communicate-spies.html?ns_mchannel=rss&ns_campaign=1490&ito=1490> - Please view link - unable to able to access data
2. <https://www.theguardian.com/us-news/2022/sep/29/cia-websites-security-sources-communication-safety> - A report found that the CIA used hundreds of covert websites for communication, which were severely flawed and could have been identified by even an 'amateur sleuth'. These flaws reportedly led to the death of more than two dozen US sources in China in 2011 and 2012 and also reportedly led Iran to execute or imprison other CIA assets. The research was conducted by security experts at the Citizen Lab at the University of Toronto, which started investigating the matter after it received a tip from reporter Joel Schectmann at Reuters.
3. <https://www.overtdefense.com/2022/10/05/poorly-designed-cia-websites-likely-got-spies-killed/> - Citizen Lab, a University of Toronto laboratory, identified a network of 885 websites used by the CIA to covertly communicate with spies abroad. However, the sites were designed in an extremely flawed manner and likely enabled the Chinese and Iranian regimes to easily detect and capture individuals spying for the United States. The weakness of the network may be a key reason behind China’s success in neutralizing the US spy network in China in 2011-2012.
4. <https://gizmodo.com/cia-websites-reportedly-led-to-the-exposure-of-critical-1849601326> - The CIA's covert communication system, which relied on hundreds of websites designed to appear as legitimate news, weather, and healthcare sites, was reportedly compromised due to its easily identifiable flaws. This led to the exposure of critical assets, including the death of more than two dozen sources in China and the execution or imprisonment of other CIA assets in Iran. The system's flaws were reportedly so severe that even an 'amateur sleuth' could have identified the network.
5. <https://www.theguardian.com/us-news/2022/sep/29/cia-websites-security-sources-communication-safety> - A report found that the CIA used hundreds of covert websites for communication, which were severely flawed and could have been identified by even an 'amateur sleuth'. These flaws reportedly led to the death of more than two dozen US sources in China in 2011 and 2012 and also reportedly led Iran to execute or imprison other CIA assets. The research was conducted by security experts at the Citizen Lab at the University of Toronto, which started investigating the matter after it received a tip from reporter Joel Schectmann at Reuters.
6. <https://www.overtdefense.com/2022/10/05/poorly-designed-cia-websites-likely-got-spies-killed/> - Citizen Lab, a University of Toronto laboratory, identified a network of 885 websites used by the CIA to covertly communicate with spies abroad. However, the sites were designed in an extremely flawed manner and likely enabled the Chinese and Iranian regimes to easily detect and capture individuals spying for the United States. The weakness of the network may be a key reason behind China’s success in neutralizing the US spy network in China in 2011-2012.
7. <https://gizmodo.com/cia-websites-reportedly-led-to-the-exposure-of-critical-1849601326> - The CIA's covert communication system, which relied on hundreds of websites designed to appear as legitimate news, weather, and healthcare sites, was reportedly compromised due to its easily identifiable flaws. This led to the exposure of critical assets, including the death of more than two dozen sources in China and the execution or imprisonment of other CIA assets in Iran. The system's flaws were reportedly so severe that even an 'amateur sleuth' could have identified the network.