The United States Department of Justice

FOR IMMEDIATE RELEASE
WWW.JUSTICE.GOV/NEWS

October 29, 2026

Syrian Man Sentenced for Wide-Ranging Hacking Conspiracy Conducted on Behalf of the Bashar Al Assad Regime

Ahmad Umar Agha (also known as Th3Pr0) had spent more than a decade as a fugitive for targeting of Western media entities, businesses, NGOs, and U.S. and allied government entities

WASHINGTON — Today a federal district court in the Eastern District of Virginia sentenced Ahmad Umar Agha to 42 months in prison for his central role in an expansive hacking conspiracy organized and led by members of former Syrian President Bashar Al-Assad's inner circle, including the commander of Syria's General Intelligence Directorate, from as early as Aug. 24, 2011, to Jan. 31, 2024.

To spread the former Syrian government's propaganda, Agha hacked approximately 47 Western media entities, businesses, non-governmental organizations (NGOs), and U.S. and allied government entities. The hacking conspiracy penalized the free press for reporting on the former Syrian government's atrocities during the Arab Spring and subsequent Syrian Civil War; used information warfare tactics to cause fear and confusion among Syrian government opponents; collected intelligence for the former Syrian government; and attempted to cause mutiny or refusal of duty by members of the military of the United States. In one instance, Agha's actions caused a flash crash in the U.S. stock market, resulting in a temporary $136 billion loss in the value of stocks making up the Dow Jones Industrial Average.

"Agha deployed his hacking skills in the service of Assad's regime to silence reporting on the regime's atrocities, intimidate its opponents, and incite U.S. servicemembers to refuse their orders," said Assistant Attorney General for

National Security John A. Eisenberg. “His attacks on our networks and institutions, including one that temporarily erased $136 billion from U.S. investors, constitute an assault on the free press and our national and economic security. Today’s sentence should serve as a reminder of the National Security Division’s long memory in pursuit of state-sponsored hackers such as Agha.”

“This case emphasizes the grave threat posed by cyber criminals and especially those serving regimes hostile to the United States,” said First Assistant U.S. Attorney Theophani K. Stamos for the Eastern District of Virginia. “The protection of our electronic infrastructure, financial markets, and the companies that serve the American people is of paramount importance. We will pursue and prosecute anyone who endangers the systems that reinforce our national security or undermines the institutions on which our people rely.”

“Today’s sentence sends a clear message that those who target American institutions, journalists, and government entities with malicious cyber activity will be held accountable, no matter how long they attempt to evade justice,” said Assistant Director in Charge Darren B. Cox of the FBI Washington Field Office. “For years, Agha conducted intrusions designed to spread disinformation, steal data, and intimidate victims on behalf of the former Syrian regime, and then spent a decade as a fugitive. The FBI Washington Field Office, together with our partners across the Department of Justice and the FBI, remained steadfast in pursuing this case and ensuring that those who threaten U.S. institutions are brought to justice.”

According to court filings, Agha’s criminal scheme forced many of his victims to spend significant sums of money remediating these intrusions or restructuring their security. Notable examples of Agha’s successful hacks include:

- Company G, a company that provides online publishers with content, website ads, and links to other websites, suffered a loss of approximately $35,000 a day for approximately six months.
- One global NGO was forced to deploy a new suite of network monitoring products – costing around $250,000 – in addition to retraining over 800 staff members and upgrading its security system. In total, the NGO suffered a total of $480,000 in losses.
- Agha’s hack of the Twitter account of a widely respected news agency allowed him to make an April 23, 2013, Twitter post falsely claiming that President Obama was injured after two explosions at the White House. Agha’s actions caused a temporary $136 billion flash crash in the value of stocks making up the Dow. Agha later bragged about this hack in an interview with Business Insider, stating that it “was our goal of that hack attack” for the Dow to drop significantly, and “it was a big victory for us.”
- Agha obtained access to the company hosting the U.S. Marine Corps’ recruitment website and redirected visitors from that site to a server

displaying an image encouraging Marines to refuse their orders and fight alongside the Syrian Army, as shown below:



Image encouraging Marines to refuse their orders and fight alongside the Syrian Amy

- During the time the attack took place, approximately 3,500 potential visitors to the U.S. Marines recruitment website saw the above image instead of U.S. Marines-related recruitment material.
- On two occasions, Agha attempted to obtain control over the White House's social media page by stealing usernames and passwords for the email accounts of White House staff. In one instance, Agha succeeded and used his unauthorized access in an unsuccessful effort to trick other White House Staff into giving him access to the White House's social media accounts.

Agha and his coconspirator, Firas Dardar, were indicted on May 17, 2018, after initially being charged by complaint on June 12, 2014. Dardar remains a fugitive. Dardar was also charged in a separate conspiracy in the Eastern District of Virginia on Sept. 29, 2015, relating to unauthorized access to, and damage of, computers and related extortionate activities; receiving the proceeds of extortion; money laundering; wire fraud; violations of the Syrian Sanctions Regulations; and unlawful interstate communications, alongside Peter Romar, a Syrian national then residing in Germany. Romar was extradited to the Eastern District of Virginia from Germany and pleaded guilty on Sept. 28, 2016.

The FBI's Washington Field Office investigated the case, in coordination with the FBI's Cyber Division.

Assistant U.S. Attorney Laura D. Withers for the Eastern District of Virginia and Trial Attorney Jacques Singer-Emery for the National Security Division's National Security Cyber Section prosecuted the case.

###

NSD

26-1289

Do not reply to this message. If you have questions, please use the contacts in the message or call the Office of Public Affairs at 202-514-2007.