

Another Israeli Spy Story: When Will It End?

One wonders when the penny will drop and the American people will rise up and say “enough is enough,” Philip Giraldi writes.

By [Philip Giraldi](#)

Global Research, July 30, 2021

[Strategic Culture Foundation](#) 29 July 2021

Region: [Middle East & North Africa](#)

Theme: [Intelligence](#)

All Global Research articles can be read in 51 languages by activating the “Translate Website” drop down menu on the top banner of our home page (Desktop version).

Visit and follow us on Instagram at [@crg_globalresearch](#).

It is perhaps not necessary to point out how the mainstream media in the United States as well as in Europe and Oceania persist in ignoring or otherwise covering up stories that make the Israelis look bad. Recent accounts of the slaughter of children and mostly civilians in Gaza by Israeli planes, missiles and artillery consistently try to depict the conflict as warfare between two comparable opponents, ignoring the enormous disparity in the military force available to the two sides. Israel has a modern army, air force and navy while Hamas has nothing but some small arms as well as improvised rockets and incendiary balloons.

The reluctance to criticize Israeli behavior is largely attributable to the power of the Zionist lobbies in the respective countries but it is also at least in part due to the complicity of Western governments in conniving at the Jewish state’s actions in its own region. **The persistence in Israeli demands for war against Iran, preferable fought by the United States, was clear again this past week** when the new government in Jerusalem declared that it would be [increasing its military budget](#) in anticipation of war with the Islamic Republic. Perhaps not surprisingly, the U.S. Congress also has several bills pending that would increase military assistance to Israel by a factor of three.

Aside from their overwhelming affection for the Jewish state, politicians and talking heads in Washington have always sought to have an enemy to explain why the foreign and national security policies have been such failures. Russia was so designated during the long years of the Cold War and more recently both the White House and Congress have begun to warn that it is China that is seeking to confront democratic norms and “export its authoritarian model.”

Given all of that, there must have been shock in a number of newsrooms when it turned out that the guilty party behind an explosive spy story that was revealed recently appears to be none other than America’s “closest ally and best friend.” It seems that a private Israeli surveillance plus security firm consisting of former cyberwarfare military and intelligence officers and having close ties to the Benjamin Netanyahu government has been selling advanced spyware to at least 45 governments. The sales are in theory restricted for use only in terrorism and criminal cases, but somehow the resource has instead been routinely

used against journalists, political activists, business executives, and politicians. Saudi Arabia, for example, [used the spyware](#) to track dissident journal Jamal Khashoggi, who was murdered by Saudi agents in Istanbul in 2018.

And even though the software has been regularly used against U.S. government officials and journalists, it appears that the Biden Administration has been aware of its capabilities and has done nothing to stop it. In its own defense, the Israeli company NSO that developed the spyware has claimed, implausibly, that it can no longer be used to hack U.S. phones. That assertion [was debunked](#) by former NSA whistleblower **Edward Snowden**, who tweeted “NSO’s claim that it is ‘technologically impossible’ to spy on American phone numbers is a bald-faced lie: a exploit that works against Macron’s iPhone will work the same on Biden’s iPhone. Any code written to prohibit targeting a country can also be unwritten. It’s a fig leaf.”

The [surprise revelation](#) of the Israeli activity came not from a government counter-intelligence agency, but rather from a group of 17 international media organizations that formed a consortium to investigate a data leak relating to hacked telephones. The group included major news outlets that had apparently been targeted using the Pegasus hacking spyware developed by the NSO Group, which was primarily designed to penetrate the security features of smartphones. One former cybersecurity engineer from the U.S. intelligence community [described Pegasus](#) as an “eloquently nasty” tool that could be used to “spy on almost the entire world population.” The spyware “can be installed remotely on a targeted person’s smartphone [without requiring them to take any action](#) such as clicking on a link or answering a call. Once installed, it allows clients to take complete control of the device, including accessing messages from encrypted messaging apps like WhatsApp and Signal, and turning on the microphone and camera.” It can also reveal the phone’s location.

The software was designed [with a backdoor](#) which allowed NSO to monitor the surveillances and it is [presumed that](#) the information was also shared with Israeli intelligence. [By one estimate](#) 50,000 smartphones were accessed worldwide, including 10 prime ministers, three presidents [including Emmanuel Macron of France](#), a king, foreign ministers and assorted journalists and government officials both in the U.S. and elsewhere.

A more cautious estimate from the *Washington Post*, [which participated in the investigation](#), states only that “1,000 people spread across 50 different countries were identified as having numbers on the list, [among them](#) are ‘several Arab royal family members, at least 65 business executives, 85 human rights activists, 189 journalists, and more than 600 politicians and government officials.’ This [includes](#) Robert Malley, the Biden administration’s lead Iran negotiator, and journalists for CNN, the Associated Press, the *Wall Street Journal*, and the *New York Times*.” Other news agencies that were hacked by Pegasus include Agence France-Presse, Al Jazeera, France 24, Radio Free Europe, Mediapart, El País, the Associated Press, Le Monde, Bloomberg, the Economist, Reuters and Voice of America.

Some are inevitably wondering why the Biden White House has been silent about NSO. It has not identified the Israeli firm as a threat to national security and made demands to the Israeli government that it intercede with NSO and shut down the use of Pegasus until some international regulation of the use of hacking software can be developed. Part of the [explanation for the reluctance](#) might be that Biden’s senior adviser Anita Dunn’s consulting firm SKDKickerbocker was hired by NSO in 2019 to provide “public relations” advice to improve the company’s image.

The reluctance, of course, also derives from the fact that Israel is involved, but those with longer memories of the Jewish state's record in stealing American secrets should not be surprised by this latest venture. Israeli-recruited U.S. Navy analyst Jonathan Pollard was, for example, the most damaging spy in U.S. history. And Israel has, in fact, a long history of stealing U.S. technology and military secrets to include sharing them with countries that Washington has regarded as enemies, including China and Russia.

Israel [always features prominently](#) in the annual FBI report called *Foreign Economic Collection and Industrial Espionage*. The 2005 report states: "Israel has an active program to gather proprietary information within the United States, these collection activities are primarily directed at obtaining information on military systems and advanced computing applications that can be used in Israel's sizeable armaments industry." It adds that: "Israel recruits spies, uses electronic methods, and carries out computer intrusion to gain the information." A 1996 Defense Investigative Service report noted that: "Israel has great success stealing technology by exploiting the numerous co-production projects that it has with the Pentagon." It says: "Placing Israeli nationals in key industries is a technique utilized with great success." A General Accounting Office (GAO) examination of espionage directed against American defense and security industries described how: "Israeli citizens residing in the U.S. had stolen sensitive technology to manufacture artillery gun tubes, obtain classified plans for reconnaissance systems, and pass sensitive aerospace designs to unauthorized users." The GAO concluded that: "Israel conducts," and this is a quote, "conducts the most aggressive espionage operation against the United States of any U.S. ally." More recently, FBI counterintelligence officer John Cole has reported how many cases of Israeli espionage are dropped under orders from the Justice Department. He has provided a conservative estimate of 125 viable investigations into Israeli espionage — involving both American citizens and Israelis — that were stopped due to political pressure.

So Israel gets yet another pass on its spying against the United States. Indeed, the Biden Administration has yet to definitively comment on the latest impropriety. One wonders when the penny will drop and the American people will rise up and say "enough is enough."

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram, @crg_globalresearch. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Philip M. Giraldi, Ph.D., is Executive Director of the Council for the National Interest, a 501(c)3 tax deductible educational foundation (Federal ID Number #52-1739023) that seeks a more interests-based U.S. foreign policy in the Middle East. Website is <https://councilforthenationalinterest.org> address is P.O. Box 2157, Purcellville VA 20134 and its email is inform@cnionline.org

He is a frequent contributor to Global Research.

The original source of this article is [Strategic Culture Foundation](#)
Copyright © [Philip Giraldi](#), [Strategic Culture Foundation](#), 2021

[Comment on Global Research Articles on our Facebook page](#)

Become a Member of Global Research

Articles by: **Philip Girdi**

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca