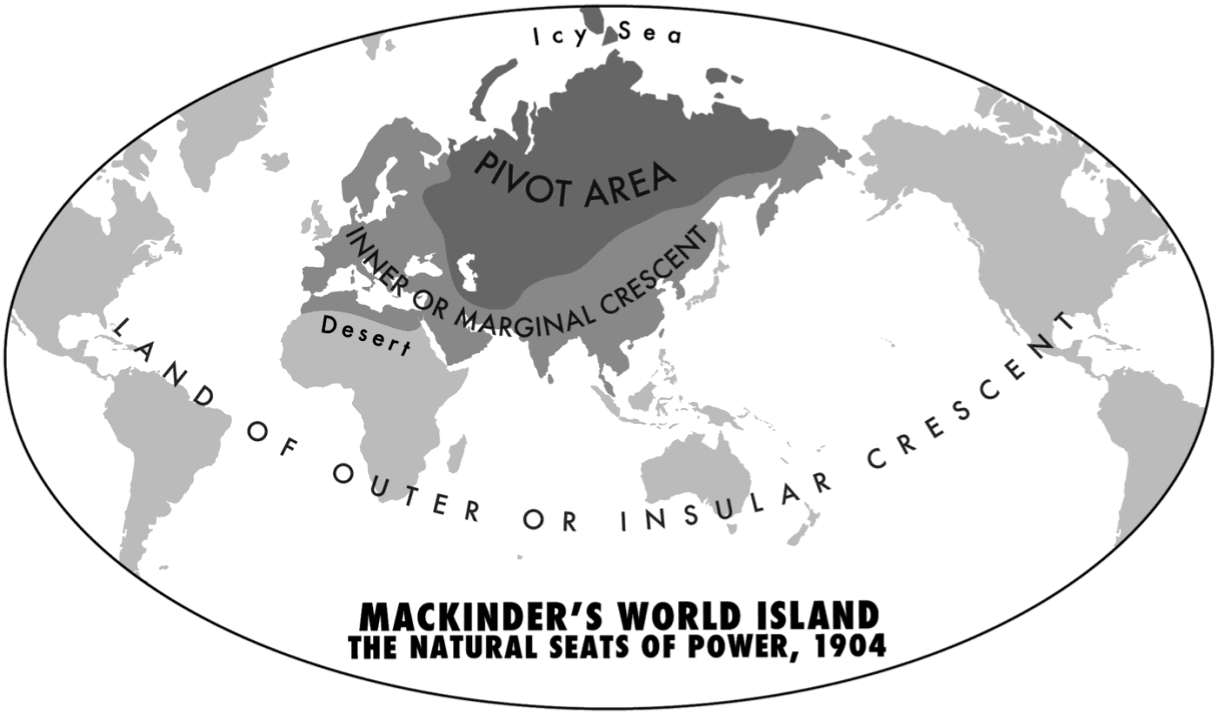
Icy Sea
PIVOT AREA
INNER OR MARGINAL CRESCENT
Desert
LAND OF OUTER OR INSULAR CRESCENT
MACKINDER'S WORLD ISLAND
THE NATURAL SEATS OF POWER, 1904

Who rules East Europe commands the Heartland;
who rules the Heartland commands the World-Island;
who rules the World-Island commands the world.

— Mackinder, Democratic Ideals and Reality, p. 150

UK CRITICAL INFRASTRUCTURE: THE RISKS OF PARTNERING WITH THE ISRAELI STATE

Written by:

D. Calderón

U.S. Army Veteran

Dear

As your constituent I demand you read the following document and take appropriate action based on the suggestions listed:

Executive Summary

Many have heard of the Chinese and Russian involvement in the Belt and Road Initiative (BRI), but few know of Israel's central role in the new "multipolar world" or understand the ramifications for critical infrastructure. The purpose of Russia seizing Ukraine is to establish Mackinder's World Island. BRI's goal for Israel as the technological hub is to provide data from fiber optic cables that will intersect Africa, Asia, and Europe (Lin 2016). In 2017, during the Beijing summit, Chinese Vice Premier Liu Yangong and Israeli Prime Minister Benjamin Netanyahu agreed to "bring the ties and the cooperation between the two countries to new heights." Netanyahu also stated, "We want to marry our technology with China's capacity" (Ahren 2017). The UK's Ministry of Defense is wary of Russia, especially after the start of the war in Ukraine, but willfully ignores Israel's long history of close economic and military ties. Current laws and sanctions recognize the Russian threat but completely overlook the Israeli government's close connections to both Russia and China. After the initial Russian sanctions, at least fourteen Russian oligarchs fled to Israel to hide from the penalties. The Russian Israeli faction of the Israeli government has close ties with both Russia and Vladimir Putin. The Ministry of Defense must recognize those close ties and limit their access to Britain's critical infrastructure.

Key Messages

- 2030 Roadmap for Israel-UK Bilateral Relations promotes Israel to a 'Tier 1' cyber partner.
- Israeli spyware led to the murder of journalist Jamal Khashoggi and targeted activists, academics, government officials, and Prime Minister Boris Johnson's office.
- Israel has a long history of stealing technology from the US, then on-selling it to Russia and China.
- Israel's IDF Talpiot Program and Unit 8200 intelligence veterans populate cybersecurity companies contracting with the government to secure critical infrastructure.
- The Talpiot Program is populated by Russian Israelis who mostly don't qualify or identify as Jewish under halakha law.
- Israel refuses to adopt all EU sanctions against Russia. Israeli diamond traders are aiding Russia in bypassing sanctions and funding Putin's war on Ukraine.
- Intel x86 processor hardware backdoors override all security settings. Intel Corporation's CPU design and fabrication facility is in Israel.

Background

Israeli and Jewish journalists wrote about the effects the mass immigration of Soviet "Aliyah" with loose immigration requirements for decades. According to Israel's Central Bureau of Statistics, "around 30% of immigrants from the former Soviet Union in the 1990s were not Jews or not considered Jewish under Orthodox law. In 2005, that figure leapt to 59%. Only around 5% of the non-Jews have converted" (Sherwood 2011). Lilly Galili, an opinion piece writer for *The Guardian*, described the high technology industry in Israel as dominated by Russian and Ukrainian computer scientists, missile technicians, aeronautical engineers, and materials scientists. "It was a very different type of immigration," stated Ms. Galili. "They didn't want to integrate. They wanted to lead. They changed the nature of the country." She pointed to “some sense of alienation between Russian immigrants and native-born Israelis. There is not much social interaction. There are still places for ‘Russians’ that ‘Israelis’ don’t go and aren’t wanted – and vice versa” (Sherwood 2011). The ultra-orthodox are exempt from mandatory military service in the Israeli Defense Forces, leaving only 10% of servicemembers with an orthodox background. Most of the Israeli Defense Forces are from the former Soviet Union or the children of Soviet immigrants with close ties to Russia.

Israeli - Russian Immigrant Antagonism

The conflict between Russian immigrants and the Orthodox community is exemplified by Israeli politician Avigdor Lieberman. He is the founder of the secular Yisrael Beiteinu (Israel is Our Home) party, whose base is overwhelmingly Russian-speaking immigrants, and he is regarded as a “kingmaker” in Israel’s coalition government. Lieberman’s disdain for religious Jews was apparent when he stated, "I will send the haredim, together with Netanyahu, in one wheelbarrow to a garbage dump” (Shaul 2021). During a 2009 visit to Moscow, Lieberman "behaved like an old friend," said Israeli delegate Yuval Fuchs, and noted that the Russians "acted as if they already knew him," according to a Wikileaks document (JPost 2010). Lieberman’s close ties with the Kremlin concerned many in Israel, who accused him of being an agent of Russia.

The ‘Backdoor Conduit’ to Russia

Soviet immigrants are populating Israel’s Talpiot Program and Unit 8200 (NSA equivalent) that produce high technology CEOs, placing them all over the world, including the UK. The Talpiot Program is an elite Israeli Defense Forces training program using their expertise to further IDF technological research. They train under Israeli military intelligence for at least 7-10 years. It is surprising government officials have failed to grasp and address the Israeli state as a “backdoor conduit” for illegal high technology transfers to Russia. This is an open-door for Russian GRU (military intelligence) and SVU (KGB) infiltration of American and British high technology sectors via easy Israeli visas and citizenship. Elements within Israeli intelligence have warned that the Israeli government is heavily penetrated by Russian assets (Aderet 2016). Thus, Russian penetration of the United Kingdom’s critical infrastructure has come through Israel’s Talpiot Program and Unit 8200 military intelligence.

Eugene Kaspersky – head of the Russian cybersecurity firm Kaspersky Lab – has partnered with the “Jerusalem municipality and others in Israel” as a center of cyber-security technology (Shamah 2016b). Kaspersky has alleged ties to Russian intelligence due to his education at a KGB-sponsored technical college and his work for the Russian military; in 2017, the Trump administration banned Kaspersky software from government computers (Free Russia Forum n.d.). The day after Russia invaded Ukraine, the U.S. government privately warned American companies that “Moscow could manipulate software designed by Russian cybersecurity company Kaspersky to cause harm,” according to a senior U.S. official (Bing 2022).

At the recent G7 Summit, Ursula von der Leyen described the negations of the 11th round of sanctions as “aimed at closing loopholes and tackling circumvention” on third-party countries (Tidey 2023). The new measures would allow them to penalize companies and countries that are believed to aid Russia in bypassing sanctions. Despite Israel’s promise not to be a ‘dirty money haven’ for Russia, Israeli diamond traders are funding Putin’s war through a loophole in US law allowing traders to sell Russian diamonds if they come via Israel (Megiddo 2022). Five Israeli companies are still working with Russian diamond firm Alrosa to sidestep sanctions. Lev Leviev who immigrated to Israel in 1971 from the former Soviet republic of Uzbekistan, is known as the “king of diamonds.” Leviev has close ties to Vladimir Putin, and fled to Moscow after he was accused of smuggling, money laundering, and tax offenses in Israel (Heller 2018).

Israel’s ‘Secret Sauce’

British intelligence and tech sector leaders claim they have much to learn from Israeli expertise despite their spying and human rights abuses. Most of Israel’s “expertise” comes from either stolen US technology or the Binational Industrial Research and Development Foundation, which jointly funds US and Israeli technology research and development. In the 1950s, Israel built a nuclear bomb using technology and materials stolen by a network of agents from the United States; all the while, the western governments in the UK and US turned a blind eye (Borger 2014). In 2007, the Americans flagged Israel as a top spy threat, according to the NSA (Stein 2014). Israel’s stealing of U.S. high technology and on-selling it to enemies in China and Russia is well documented and reported (Military.com 2013). Israel’s technology innovation comes from the United States, not the Talpiot Program.

Israel’s Espionage and Influence Operations

In 2017, Al Jazeera filmed an Israeli embassy official, Shai Masot, plotting to “take down” MPs regarded as hostile due to their support of Palestine, such as Alan Duncan and Jeremy Corbyn. Masot set up several pro-Israel political organizations in the UK that intended to influence Labour Party policy while appearing to obscure their links to the state of Israel (MacAskill 2017). Masot’s LinkedIn profile stated, “founding several political support groups in the UK to maximise the Israeli ‘firewall’”. He also claimed to have secured “adjustments to legislation” in the UK. In 2021, the British Labour Party appointed a former Israeli intelligence operative, Assaf Kaplan, to work in the office of Keir Starmer. Kaplan’s past employment profile highlights his years spent in the infamous Unit 8200, which has a long record of surveilling Palestinians and human rights abuses. One of the unit’s missions, publicized by whistleblowers in 2014, is to blackmail individual Palestinians and threaten them into collaborating with the Israeli military against fellow Palestinians. Kaplan was also a friend of the disgraced Shai Masot (Cook 2021).

Cyber espionage firms such as NSO Group, Candiru, Black Cube, and others are heavily recruited from Unit 8200 to develop powerful cyber weapons (MacLeod 2022). This predominately unregulated spyware market will take more than blacklisting to rein in these companies when Israel’s private sector and military intelligence are intimately intertwined. The military and private sector in Israel allowed dangerous cyber weapons like NSO’s Pegasus and Candiru spyware to flourish worldwide. In 2018, Pegasus unequivocally aided in journalist Jamal Khashoggi’s murder (TOI Staff 2021). In the summer of 2020, the UK Prime Minister Boris Johnson’s office and multiple devices at the Foreign Commonwealth and Development Agency were targeted by Israeli made spyware. A watchdog group, Citizen Lab, issued an in-depth report on NSO Group’s spyware targeting activists, academics, and government officials. "People think that the problem with mercenary spyware is that it is sold to dictators who abuse it. True. But even when spyware like Pegasus is sold to democracies, it gets abused," Citizen Lab wrote in the report (Kan 2022).

Unit 8200 whistleblowers are coming forward to expose Israel’s unethical behavior, not only towards the Palestinians, but also against American and European citizens**. “We spent our time essentially carrying out surveillance of a civilian population who had no access to legal counsel and were denied civil rights,”** G [anonymous Unit 8200 veteran] said of his experience in Israeli army intelligence. **“We were trained to violate people’s privacy for a living, and then were offered even more money to do it abroad”** (Goodfriend 2021).

Context of the Issue

Over the past couple of decades, more than 400 Israeli tech firms have operated in the country. Most of the legislation to protect critical infrastructure focuses on sanctions and laws against countries that partner with Israel on the BRI but does not tackle the threat of Israel itself. What is most concerning is legislation mandating Israel as a 'Tier 1' cybersecurity partner and prioritizing increased links between Israeli startups and the UK sector. Sanctions should apply to Russian Israelis, and Israel must hold accountable Russian oligarchs who hold dual Russian and Israeli citizenship. Israel has refused to cooperate on all the sanctions, and diamond trader loopholes are aiding Vladimir Putin's war against Ukraine (Megiddo 2022).

1. **2030 Roadmap for Israel-UK Bilateral Relations**

   Promises ongoing cooperation in tackling cyberthreats, governing global cyberspace, developing cybersecurity skills, and investing in the cybersecurity ecosystem.

   Includes joint commitments in areas such as technology, innovation, research and development in national security aim to enable both countries to remain at the forefront of the technological revolution.

2. **Providing Professional and Business Services to a Person Connected with Russia**

   Regulation 54C of the Russia (Sanctions) (EU Exit) Regulations 2019 prohibits a legal or natural person from providing, directly or indirectly, accounting, advertising, architectural, auditing, business and management consulting, engineering, IT consultancy and design, and public relations services to a 'person connected with Russia'.

Scope of the Problem

An emerging industry narrative contained in online journals and news articles speaks boldly of Israel's cyber technology defense—hardware and software. The general mainstream discourse rarely touches on the security implications of this move. Few in the intelligence and IT industries know that core technology components of the emerging 5G, IoT artificial intelligence world, Microsoft Windows security center, and other core components are key coded in Israel. Here are just a few of the critical infrastructure contracts with Israeli companies with ties to the Talpiot Program and/or Unit 8200:

1. **RAD Group:** founded by Talpiot Program graduate and Unit 8200 veteran Zohar Zisapel. Provider for more than 100 telecom operators worldwide and critical infrastructure in the banking, commerce, education, finance, government, military, transportation, and utility sectors.

2. **Carbyne 911:** a next-generation 911 program that was reverse-engineered by Human Rights Watch, which determined the application is similar to China's "integrated Joint Operations Platform" that's used for mass surveillance of the Uyghurs (Bensaid 2019).

3. **Elbit Systems:** The UK Ministry of Defense approved a $71 million contract for the Ground Manoeuvre Synthetic Trainer Systems (GMST) for the Boxer armored vehicles and Challenger 3 tanks under the British Army's Project Vulcan. The Australian Army canceled their contract over concerns of backdoors,

followed later by the Australian Future Fund over the allegation that Israel gave Russian forces cluster munitions used during the invasion of Ukraine (Middle East Monitor 2021)

4. **Verint:** provider for the entire UK police forces as part of Project IRIS to support evidence capture, internet connectivity, and auditing. Project IRIS represents all police forces in England and Wales as well as associated forces and agencies across the UK, including Police Scotland and the Police Service of Northern Ireland.

5. **Microsoft:** The Ministry of Defense (MOD) adopted the Microsoft Cloud, as well as Office 365 Advanced Threat Protection and Customer Lockbox. Core coding is handled in Israel and not in the United States (Shamah 2016a). The former head of Microsoft Israel, Assaf Rappaport, was Israeli military intelligence trained under their elite Unit 8200 and Talpiot Program.

6. **QualComm Snapdragon:** M2M (machine-to-machine) mobile platform, which is used to track the location of pets, children, the elderly, and expensive goods, was largely developed in Israel.

7. **Intel CPU:** the x86 processors contained hardware backdoors called "God Mode," overriding all security settings. The design and fabrication facilities are in Israel and directly tied to Israeli technicians. The current Intel 10nm "disaster" is speculated to involve "design flaws" that cannot be micro-coded around in the short term. (News18 2020).

In 2018, U.S.-based cyber security researcher Christopher Domas spoke at a Black Hat USA conference. He elaborated on his research into the DEC (deeply embedded core) present in Intel processors that allowed total access to a targeted system. The DEC can be activated via multiple machine code instruction sets and bypasses all hardware and software security (Black Hat USA 2018). There's intense speculation that this hardware backdoor was conceived and implemented in Israel.

Recommendations

In order to secure the United Kingdom's critical infrastructure from Chinese and Russian attacks, government officials must address Israel's special treatment by politicians funded and influenced by foreign political lobbies.

1. All critical infrastructure contractors should require full background checks and a ban on employees with foreign military ties from directly working on cybersecurity projects.

2. Add Russian Israelis with ties to Russia to the EU's sanctions.

Conclusion

Large sections of the Israeli state and Jews in general are not knowingly involved in such deep and very public deceit. The mostly non-Jewish Russian Israeli faction and the Russian oligarchs with dual Russian-Israeli citizenship are threats to the West. Russian immigrants infiltrating Israel's Talpiot Program and placing their CEOs all over the world are a 'backdoor conduit' for Russia. Israeli intelligence veterans have targeted UK politicians with influence and sabotage operations to remove MPs from office, and it would be unethical to grant them access to secure critical infrastructure. It is hypocritical to hold Russians in the West accountable for the war in Ukraine but not secular Russians in Israel. The Russian penetration of Israel and their theft of

American technology, then on-selling it to China and Russia, also make Israel a hostile foreign power to the United Kingdom.

References

Aderet, Ofer. 2016. “Secret Files Expose KGB Spies in Israel’s Top Political and Military Echelon.” *Haaretz,* Accessed January 30, 2023. https://www.haaretz.com/israel-news/2016-10-26/ty-article/files-expose-kgb-spies-in-israels-top-political-and-military-echelon/0000017f-e152-df7c-a5ff-e37a51020000

Ahren, Raphael. 2017. “In Beijing, Netanyahu looks to ‘marry Israel’s technology with China’s capacity.’” *The Times of Israel, Accessed January 30, 2023.* https://www.timesofisrael.com/in-beijing-netanyahu-looks-to-marry-israels-technology-with-chinas-capacity/

Ahren, Raphael. 2019. “Israel and Iran both set to join Russia-led free trade zone.” *The Times of Israel, Accessed January 30, 2023.* https://www.timesofisrael.com/israel-and-iran-both-set-to-join-russia-led-free-trade-zone/

Bensaid, Adam. 2019. “Two American billionaires and their shady deals with Israeli intelligence.” *TRT World, Accessed January 30, 2023.* https://www.trtworld.com/magazine/two-american-billionaires-and-their-shady-deals-with-israeli-intelligence-28819

Bing, Christopher. 2022. “EXLUSIVE U.S. warned firms about Russia’s Kapersky software day after invasion.” *Reuters, Accessed January 30, 2023.* https://www.reuters.com/technology/exclusive-us-warned-firms-about-russias-kaspersky-software-day-after-invasion-2022-03-31/

Black Hat USA. 2018. “GOD MODE unlocked: Hardware backdoors in x86 CPUs.” Youtube.com. Accessed January 30, 2023. https://www.youtube.com/watch?v=_eSAF_qT_FY

Butler, Ben. 2022. “Australia’s Future Fund bans investment in Israeli defense contractor over cluster munitions allegations.” *The Guardian, Accessed January 30, 2023. https://www.theguardian.com/world/2022/mar/10/elbit-systems-denies-making-cluster-bombs-after-australia-future-fund-bans-investment-in-it*

Baroud, Ramzy. 2022. “Why China and Russia seek a ‘Multipolar World Order.’” *Gulf News,* Accessed January 30, 2023. https://gulfnews.com/opinion/op-eds/why-china-and-russia-seek-a-multipolar-world-order-1.87120017

Borger, Julian. 2014. “The truth about Israel's secret nuclear arsenal.” The Guardian, Accessed May 16, 2023. https://www.theguardian.com/world/2014/jan/15/truth-israels-secret-nuclear-arsenal

Cook, Jonathan. 2021. “Former Israeli army spy recruited by Labour will feel right at home.” Middle East Eye, Accessed May 16, 2023. https://www.middleeasteye.net/opinion/former-israeli-army-spy-recruited-labour-will-feel-right-home

Heller, Aron. 2018. “Diamond smuggling scandal spotlights shadowy Israeli tycoon Lev Leviev.” *The Times of Israel*, Accessed May 16, 2023. https://www.timesofisrael.com/diamond-smuggling-scandal-spotlights-shadowy-israeli-tycoon-lev-leviev/

Lin, Christina. 2016. “Bunting’s map and Israel on China’s new silk road.” *The Times of Israel, Accessed January 30, 2023*. https://blogs.timesofisrael.com/buntings-map-and-israel-on-chinas-new-silk-road/

Free Russia Forum. n.d. “Putin’s List Kaspersky Evgeny.” Accessed January 30, 2023. https://www.spisok-putina.org/en/personas/kaspersky/

Frenkel, Jonathon. 2020. “WHY ARE 4 US STATES BUILDING BRIDGES TO ISRAELI TECH?” *Israel21c,* Accessed January 30, 2023. https://www.israel21c.org/why-are-4-us-states-building-bridges-to-israeli-tech/

Galili, Lily. 2020. “The other tribe: Israel’s Russian-speaking community and how it is changing the country.” *Report The Brookings Institute*, Accessed January 30, 2023. https://www.brookings.edu/research/the-other-tribe-israels-russian-speaking-community-and-how-it-is-changing-the-country/

Goodfriend, Sophia. 2021. "'We violated people's privacy for a living': How Israel's cyber army went corporate." *+972 Magazine,* Accessed January 30, 2023. https://www.972mag.com/nso-surveillance-companies-israel-army/

JPost. 2010. "Wikileaks: Russia sees Lieberman as 'one of their own.'" *The Jerusalem Post,* Accessed January 30, 2023. https://www.jpost.com/International/Wikileaks-Russia-sees-Lieberman-as-one-of-their-own

Kan, Michael. 2022. "NSO Group's Pegasus Spyware Used to Hack UK Prime Minister's Office." *PC Magazine*, Accessed May 16, 2023. https://www.pcmag.com/news/nso-groups-pegasus-spyware-used-to-hack-uk-prime-ministers-office

MacAskill, Ewen. 2017. "Israeli diplomat who plotted against MPs also set up political groups." The Guardian, Accessed May 16, 2023. https://www.theguardian.com/world/2017/jan/08/israeli-diplomat-shai-masot-plotted-against-mps-set-up-political-groups-labour

MacLeod, Alan. 2022. "REVEALED: THE FORMER ISRAELI SPIES WORKING IN TOP JOBS AT GOOGLE, FACEBOOK, AND MICROSOFT." *Mint Press News*, Accessed January 30, 2023. https://www.mintpressnews.com/revealed-former-israeli-spies-working-top-jobs-google-facebook-amazon/282413/

Megiddo, Gur. 2022. "Israeli Diamond Traders Fund Putin's War Machine in Ukraine." Haaretz. Accessed May 15, 2023. https://www.haaretz.com/israel-news/2022-04-13/ty-article-magazine/.premium/the-israeli-diamond-traders-funding-putins-war-machine/00000180-5b9d-dc66-a392-7fdfe98b0000

Middle East Monitor. 2021. "Australia military to stop using Israel defense system." Middleeastmonitor.com Accessed January 30, 2023. https://www.middleeastmonitor.com/20210505-australia-military-to-stop-using-israel-defence-system/

Military.com. 2013. "Report: Israel Passes U.S. Military Technology to China." Accessed January 30, 2023. https://www.military.com/defensetech/2013/12/24/report-israel-passes-u-s-military-technology-to-china

News 18. n.d. "Intel Patching its 'Zombieload' CPU Security Flaw for the Third Time." News18.com, Last modified January 29, 2020. https://www.news18.com/news/tech/intel-patching-its-zombieload-cpu-security-flaw-for-the-third-time-2476791.html

Shamah, David. 2016a. "Bill Gates: Israeli tech 'changing the world.'" *The Times of Israel,* Accessed January 30, 2023. https://www.timesofisrael.com/bill-gates-israeli-tech-changing-the-world/

Shamah, David. 2016b. "From Jerusalem shall come forth cyber-security, says cyber guru." *The Times of Israel,* Accessed January 30, 2023. https://www.timesofisrael.com/from-jerusalem-shall-come-forth-cyber-security-says-cyber-guru/

Shaul, Ben. 2021. "Avigdor Lieberman: 'Throw the haredim into the garbage.'" *Israel National News,* Accessed January 30, 2023. https://www.israelnationalnews.com/news/298419

Sherwood, Harriet. 2011. "Israel's former Soviet immigrants transform adopted country." *The Guardian,* Accessed January 30, 2023. https://www.theguardian.com/world/2011/aug/17/israel-soviet-immigrants-transform-country

Stein, Jeff. 2014. "Israel Flagged as Top Spy Threat to U.S. in New Snowden/NSA Document." *Newsweek,* Accessed January 30, 2023. https://www.newsweek.com/israel-flagged-top-spy-threat-us-new-snowdennsa-document-262991

Tidey, Alice. 2023. "EU to issue 'warning' to countries supporting Russia in next sanction package, VDL says." *Euro News*, Accessed May 16, 2023. https://www.euronews.com/my-europe/2023/05/15/eu-to-issue-warning-to-countries-supporting-russia-in-next-sanction-package-vdl-says

TOI Staff. 2021. "NSO's Pegasus used to target Khashoggi's wife before his murder – Washington Post." *The Times of Israel,* Accessed January 30, 2023. https://www.timesofisrael.com/nsos-pegasus-used-to-target-khashoggis-wife-before-his-murder-washington-post/