Mandate of the Special Rapporteur on extrajudicial, summary or arbitrary executions and mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Annex One

Analysis of the Evidence of Surveillance of Mr. Bezos' personal phone
- Key Technical Elements -

To complement the preliminary substantive findings and associated expressions of concern by the Special Rapporteurs to the Saudi authorities regarding their alleged surveillance of Mr. Bezos, the following annex summarises the technical methodologies deployed to establish grounds for a reasonable belief (a "medium to high confidence" to use the precise wording of the technical experts involved) that Mr. Bezos was subjected to intrusive surveillance via hacking of his phone as a result of actions attributable to the WhatsApp account used by Crown Prince Mohammed bin Salman.

An in-depth, forensic level examination of Mr. Bezos' phone – including full forensic imaging and analysis - was undertaken by a team of digital forensic experts. According to the expert team, this forensic study was undertaken in a protected environment specifically created to enable thorough investigation of the phone without risk of contamination. A full report of the expert findings was made available to the Special Rapporteurs.

The phone in question underwent the following tests:

Test undertaken	Tool used	Finding/result
Logical mobile acquisition	Cellebrite UFED 4PC	Acquisition successful
Network package collection while device was locked, unlocked, idle and while simulating activity	Wireshark, Fiddler	Collection of network traffic successful
Presence of malware	Cellebrite Physical Analyser	No known malware detected
Presence of conventional or typical malicious software	Cellebrite Physical Analyser; use of a sandboxed network to simulate an active internet connection	Vetted 350,579 unique hashes but no known malicious software detected
Presence of suspect indicators of compromise (IOCs) from the network capture logs	Cellebrite reports and captured network logs	Identified 1,290 URLs and 378 unique domain names and identified 192 potentially suspect IOCs
In-depth audit of 192 suspect IOCs	Manual review by experts	No evidence found that any of the identified domain names or URLs were related to malicious traffic.

Test undertaken	Tool used	Finding/result
Presence of jail-breaking tools and known iOS exploits tools	In-depth investigation of logical file system - auditing 274,515 directories, sub-directories and filenames	No evidence found of jail-breaking tools or known iOS exploits being present.
Analysis of suspect video file (sent to Mr. Bezos on WhatsApp from the Crown Prince's account as provided by to Mr. Bezos by the Crown Prince)	Analysis of the WhatsApp artifacts from Cellebrite reports	Initial results did not identify the presence of any embedded malicious code, but further analysis revealed that the suspect video had been delivered via an encrypted downloader host on WhatsApp's media server.
Analysis of the contents of the downloader	Attempted decryption	Due to WhatsApp's end-to-end encryption, the contents of the downloader cannot be practically determined.
Comparative analysis of cellular data egress with past usage of Mr. Bezos' phone	Analysis of the forensic artifacts from the Cellebrite reports	Records showed that within hours of receipt of the video from the Crown Prince's WhatsApp account, there was an anomalous and extreme change in phone behavior, with cellular data originating from the phone (data egress) increasing by 29,156 per cent. Data spiking then continued over the following months at rates as much as 106,031,045 per cent higher than the pre-video data egress base line.
Comparative analysis of cellular data egress with devices similar to the Bezos phone	Expert analysis of five other similar devices	Up until the day the suspect video file was received, data egress patterns were found to be similar – and explicable by nature of activity undertaken – across all five devices and Mr. Bezos' phone. Following receipt of the suspect video file, a stark contrast was found in the magnitude of data egress from Mr. Bezos' phone as compared to the five other phones.

Test undertaken	Tool used	Finding/result
Assessment of possible use of mobile spyware – cyber weapons	Expert analysis of likelihood of cyber weapons as methods for anomalous stimulation and capture of data egress	Experts advised that the most likely explanation for the anomalous data egress was use of mobile spyware such as NSO Group's Pegasus or, less likely, Hacking Team's Galileo, that can hook into legitimate applications to bypass detection and obfuscate activity. For example, following the initial spike of exfiltration after receipt of the suspect video file, more than 6GB of egress data was observed using exfiltration vectors.

Annex Two

Brief Timeline of Key Events

KEY DATE	EVENT
December 2016	At a Washington-based think-tank, Jamal Khashoggi makes critical remarks about Donald Trump's ascent to the US presidency. Soon after, the Saudi regime cancelled Mr. Khashoggi's column in the al-Hayat newspaper, and ultimately banned him from writing, appearing on television, and attending conferences. A Saudi official explained that Mr. Khashoggi's statements "do not represent the government of Saudi Arabia or its positions at any level, and his opinions only represent his personal views, not that of the Kingdom of Saudi Arabia." Mr. Khashoggi's subsequent exile from Saudi Arabia was self-imposed, based upon his belief that for his own safety and freedom he had no other choice but to leave.
September 2017	The Washington Post publishes Mr. Khashoggi's first column: "*Saudi Arabia wasn't always this repressive. Now it's unbearable.*"
November 2017	Pegasus-3 spyware is acquired from NSO Group by the Saudi regime, specifically the Saudi Royal Guard.
February 7, 2018	Washington Post publishes a column by Mr. Khashoggi entitled: "*Saudi Arabia's crown prince already controlled the nation's media. Now he's squeezing it even further.*"
February 28, 2018	Washington Post publishes a column by Mr. Khashoggi in which he writes: "…maybe [the Crown Prince] should learn from the British royal house that has earned true stature, respect and success by trying a little humility himself."
March 21, 2018	Washington Post owner, Mr. Bezos, is invited to attend a small dinner with the Crown Prince in Los Angeles.
April 3, 2018	Washington Post publishes a column by Mr. Khashoggi while the Crown Prince is in the U.S. in which Mr. Khashoggi writes: "…replacing old tactics of intolerance with new ways of repression is not the answer."
April 4, 2018	Mr. Bezos attends dinner with the Crown Prince, in the course of which they exchange phone numbers that correspond to their WhatsApp accounts.
May 1, 2018	A message from the Crown Prince account is sent to Mr. Bezos through WhatsApp. The message is an encrypted video file. It is later established, with reasonable certainty, that the video's downloader infects Mr. Bezos' phone with malicious code.
May, 2018	The phone of Saudi human rights activist Yahya Assiri is infected with malicious code. Yahya Assiri was in frequent communication with Mr. Khashoggi.

June, 2018	The phone of Saudi political activist Omar Abdulaziz is infected with malicious code, via a texted link on Whats App. Omar Abdulaziz was in frequent communication with Mr. Khashoggi.
June, 2018	The phone of an Amnesty International official working in Saudi Arabia is targeted for infection via a WhatsApp link that it is determined leads to an NSO Group-controlled website.
June 23, 2018	The phone of Saudi dissident Ghanem al-Dosari is targeted via a text link leading to NSO infrastructure.
June 23, 2018	A second phone of Saudi dissident Ghanem al-Dosari is targeted via a text link leading to NSO infrastructure.
October 2, 2018	Mr. Khashoggi is killed by Saudi government officials. The Washington Post begins reporting on the murder, publishing ever-expanding revelations about the role of the Saudi government and of the Crown Prince personally.
October 15, 2018	Massive online campaign against Mr. Bezos begins, targeting and identifying him principally as the owner of The Washington Post. In November, the top-trending hashtag in Saudi Twitter is "Boycott Amazon." The online campaign against Mr. Bezos escalates and continues for months.
November 8, 2018	A single photograph is texted to Mr. Bezos from the Crown Prince's WhatsApp account, along with a sardonic caption. It is an image of a woman resembling the woman with whom Bezos is having an affair, months before the Bezos affair was known publicly.
February 25, 2019	The Daily Beast runs an op-ed by Iyad el Baghdadi entitled "How the Saudis Made Jeff Bezos Public Enemy No. 1."
March 31, 2019	Hundreds of major news outlets around the world report on the allegation that Saudi Arabia had access to Mr. Bezos' phone and had obtained private data. The allegation was first published in a Daily Beast op-ed by Gavin de Becker, and subsequently reported by the NY Times, CNN, al Jazeera, BBC, Bloomberg, Reuters, and others.
April 1, 2019	The entire Saudi online campaign against Mr. Bezos stops abruptly, strongly indicating inauthentic and coordinated hashtags and tweets.
April 25, 2019	Intelligence officials in Norway advise Iyad el Baghdadi of a CIA warning that he is being targeted by the Saudis and move him from his home. Intelligence sources believe the threats are connected to Mr. Baghdadi's work on Jeff Bezos.
May 1, 2019	Mr. el Baghdadi is advised by a source in Saudi Arabia that the Saudis have successfully targeted his phone.
September 20, 2019	Twitter suspends 5000 accounts for "inauthentic behavior," including that of an advisor to the Crown Prince, Saud al Qahtani.
October 1, 2019	Mr. Bezos attends the memorial for Mr. Khashoggi held outside the Saudi Consulate in Istanbul where Mr. Khashoggi was murdered.
October 2, 2019	The Saudi online campaign against Mr. Bezos resumes after being dormant for months, specifically citing Mr. Bezos' attendance of the memorial event,

	and again calling for boycott of Amazon. CNN Arabia reports on the new campaign.
October 29, 2019	Facebook sues the NSO Group in U.S. federal court for trying to compromise the devices of up to 1,400 WhatsApp users' in just two weeks.
November 5, 2019	The US Department of Justice charges three people with serving as Saudi spies inside Twitter. One of the three had left Twitter and gone to work at Amazon.
November 14, 2019	Facebook confirms that "sending a specifically crafted MP4 [video] file to a WhatsApp user," is a method for installing malicious spyware; exactly as was sent to Mr. Bezos.
November 15, 2019	Several news outlets report on a WhatsApp vulnerability, and warn those who "have received a random, unexpected MP4 video file," exactly as Bezos did, to beware.
December 20, 2019	Twitter suspends 88,000 accounts linked to Saudi spying case, saying that the accounts were associated with "a significant state-backed information operation" originating in Saudi Arabia.