Graphical user interface

Description automatically generated with medium confidence

*In partnership with:*

Shape

Description automatically generated with medium confidenceText

Description automatically generated

Graphical user interface, text

Description automatically generated

**U.S. Chamber’s Delegation to Cyber Week**

**Tel Aviv, Israel**

**June 26 – 30, 2022**

**Schedule Key**

The Chamber’s delegation to Cyber Week includes official programs and events led by the US Chamber and our partners (**in black**) as well as two program tracks that delegates can choose from – cyber policy (blue) or business development (green).

* **Full Delegation (**includes official CyberWeek program, U.S. Chamber and partner events)
* **Cyber Policy Track** (including meetings with government officials, policymakers, thought leaders)
* **Practitioner Track** (including site visits, B2B meetings, networking opportunities)

**Saturday, June 25**

**7.30 p.m.** **Welcome** **Reception**

**9.00 p.m.**

**Sunday, June 26 – Site Visit to Be’er Sheva, Israel**

**9.30 a.m. Tour and Briefing of IL-CERT**

**11.00 a.m.** Israel’s Computer Emergency Response Team (IL-CERT) is Israel’s civilian center for addressing Information Security and Cyber events. It is an independent and professional organization that provides a place for people and organizations in Israel and worldwide to report events concerning the Internet in Israel. IL- CERT is responsible for coordinating activities in addressing security events, pro- active activities before they occur and information sharing and public awareness on issues of Information Security and Privacy.

**11.30 a.m. Cybersecurity Research Center at Ben Gurion University**

**12.30 p.m.** The Center harnesses the University's expertise to drive research and foster the development of cyber security technologies. The new six-floor building will be a hub of activity, largely comprised of the Department of Information Systems Engineering and the Cyber Security Research Center. The Center will include the Cyber Attack Simulation Lab, Malware Analysis Lab, Mobile Security Lab, Embedded Systems Security Lab and the Secure Cyber Lab, designated for confidential research and designed in accordance with those needs.

**1.00 p.m. Briefing with Israeli Defense Forces C4i Directorate**

**2.00 p.m.** The C4i directorate is the IDF’s elite technological unit. The main activity of the C4i directorate is to provide commanders in the field with the technology that they need in order to manage a combat situation in the best possible way. The directorate’s main objectives are to initiate, develop, exploit and strengthen the IDF’s technological integration system.

**3.00 p.m**. **Israeli National Laboratory for Cyber Security and Industrial Control Systems**

**4.00 p.m.** In collaboration with the Israeli National Cyber Directorate (INCD) of the Prime Minister’s Office, the Ministry of Energy (MoE) is establishing a national cyber security lab for research and innovation in industrial control systems (scheduled to be commercial operational by end of Q1 2022). The innovative lab facility will be a dedicated platform for simulating operational routine processes and examining scenarios, technologies, and malware. The lab’s activity will focus mainly on energy infrastructure - electricity, gas, and related areas. The lab has been defined as unclassified which will enable and encourage the use of its resources by partners in academia, research institutes, industry, manufacturers of control systems, start-up companies, and government bodies from Israel and abroad.

**6.00 p.m. Private dinner with top Israeli security/political official or journalist**

**8.00 p.m.** This dinner will focus on the changing geopolitical issues of the day in and around the Middle East.

**Monday, June 27**

**8.30 a.m. Meetings with Government Leaders and Policymakers**

**3.00 p.m.** The U.S. Chamber will convene bilateral meetings and roundtables with prominent government officials and policy makers from around the world who are attending Cyber Week.

**10.00 a.m. Visit to CyberGym**

**11:30 a.m.** CyberGym Provides tailored state of the art cyber-training solutions to organizations around the world. During this visit delegates will have the opportunity to visit CyberGym’s advanced cyber training range developing the next-generation of Israeli cyber leaders.

**12.00 p.m. Lunch with YL Ventures**

**1.30 p.m.** YL Ventures is an American-Israeli venture capital firm that specializes in seed stage cybersecurity investments. This luncheon discussion will cover the state of Israeli cyber—from amount of money raised to number of new Unicorns—the last 12-18 months have seen unprecedented growth in the Israeli cyber industry. The YL ventures team will provide a macro-overview of the current state of play in Israeli cyber as well as what they expect to see in the coming months.

**2.00 p.m. The Future of Quantum Computing**

**3.00 p.m.** Quantum computing has the potential to change the world as we know it. During this session experts

from Israel's leading quantum startups will address some of the key implications of quantum

computing. How do quantum computers actually work? Will the power of quantum make security obsolete? What are some practical applications of quantum computing? What is the current status of quantum computing and what needs to happen both technologically and policy-wise to realize quantum's potential? What is Israel's quantum strategy?

**3.30 p.m. Visit to Team8**

**5.00 p.m.** Team8 is a renowned Israeli cyber Think Tank, VC and company creation platform, founded by the former head of Israel’s legendary 8200 unit. We will start with a talk on how the renewed era of great power geopolitical competition will effect the cybersecurity of the US and its allies. Subsequently, we will breakout into working groups for sessions in key areas of cyber such as cloud, supply chain security and critical Infrastructure protection.

**6.00 p.m. Dinner with Israel’s Leading Cyber VCs and Entrepreneurs**

**8.00 p.m.** This private, curated dinner will bring togetherleading VCs and cyber entrepreneurs for networking and discussion.

**Tuesday, June 28**

**7.30 a.m. Main Plenary: The 12th Annual International Cybersecurity Conference**

**4.30 p.m.** Location: Smolarz Auditorium

**8.30 a.m. Practitioner Cluster Meetings**

**4.00 p.m.** The U.S. Chamber and our Israeli partners will curate meetings with top Israeli technology companies and startups in specific domain areas to create business-to-business opportunities for delegates. Delegates will be offered to receive their own customized pre-scheduled series of meetings with the Israeli cyber startups of their choice. We will source the best in class for cloud; API security; data protection and privacy; Zero Trust architectures; OT/IoT and more. We are also able to offer opportunities to meet Israeli startups in key emerging deep tech areas such as AI and quantum.

**8.30 a.m. Meetings with Government Leaders and Policymakers**

**4.00 p.m.** The U.S. Chamber will convene bilateral meetings and roundtables with prominent government officials and policy makers from around the world who are attending Cyber Week.

**Wednesday, June 29**

**8.00 a.m. Main Plenary: The 9th Annual International Cybersecurity Conference**

**3.30 p.m.** Location: Smolarz Auditorium

**8.30 a.m. Practitioner Cluster Meetings**

**4.00 p.m.** The U.S. Chamber and our Israeli partners will curate meetings with top Israeli technology companies and startups in specific domain areas to create business-to-business opportunities for delegates. Delegates will be offered to receive their own customized pre-scheduled series of meetings with the Israeli cyber startups of their choice. We will source the best in class for cloud; API security; data protection and privacy; Zero Trust architectures; OT/IoT and more. We are also able to offer opportunities to meet Israeli startups in key emerging deep tech areas such as AI and quantum.

**8.30 a.m. Meetings with Government Leaders and Policymakers**

**4.00 p.m.** The U.S. Chamber will convene bilateral meetings and roundtables with prominent government officials and policy makers from around the world who are attending Cyber Week.

**Thursday, June 30**

**9.00 a.m. Optional Guided Tour of Jerusalem**

**4.00 p.m.**

**9.00 a.m. Visit to Yad Vashem**

**11.00 a.m.** Yad Vashem, the World Holocaust Remembrance Center, is the ultimate source for Holocaust

education, documentation and research. From the Mount of Remembrance in Jerusalem, Yad Vashem's integrated approach incorporates meaningful educational initiatives, groundbreaking research and inspirational exhibits.

**12.00 p.m. Visit to Jerusalem’s Old City**

**3.00 p.m.** We will take a walking tour through the highlights of Jerusalem’s Old City. Follow the Byzantine Cardo through the Jewish Quarter. Visit the Western Wall, the retaining wall for the western side of the Temple Mount more than 2,000 years ago –the holiest place of prayer in Jewish tradition. Take the Via Dolorosa following in Jesus’ footsteps passing the Stations of the Cross. Visit the Church of the Holy Sepulcher, where Jesus is believed to have been crucified.

**Additional U.S. Chamber Programming Around Cyber Week**

**U.S.-Israel Cyber Forum**

* The U.S. and Israeli governments are deeply engaged in cyber cooperation across a broad range of cyber-related areas, including recent new agreements around R&D, transportation, and ransomware. There is also strong alignment on cybersecurity policies and frameworks. This forum will showcase the breadth of the U.S.-Israel cyber partnership, cooperation with the private sector, and explore new avenues for growth in this strategic pillar of the bilateral alliance.
* Potential speakers include Alejandro Mayorkas, Secretary, Department of Homeland Security, Jen Easterly, Director, U.S. Cybersecurity and Infrastructure Security Agency, Gaby Portnoy, Director General, Israel National Cyber Directorate, and Tom Nides, U.S. Ambassador to Israel.

**Dinner with U.S. Government**

* Meet with the U.S. Government delegation coming to Cyber Week from the Departments of Homeland Security, State, Energy, Treasury, the Cybersecurity Infrastructure Security Agency, and the White House.

**Roundtable: Cybersecurity risk management 2022 - between regulation, private enforcement, and markets**

* The Colonial Pipeline attack in the U.S. had a severe impact on the supply of essential public services, and once again raised the question of whether market forces are effective in influencing important private sector organizations and their leaders to prepare for cyberattacks and mitigate them. Policymakers around the world are confronting this issue. Dealing with it effectively requires developing an evidence-based policy, and effective regulatory tools in a “whole of government approach”, while trying to reduce unwanted regulatory burden. The effects of the European Union General Data Protection Regulation (GDPR) on corporate behavior also informs this discussion. This roundtable will bring together cybersecurity risk experts with policy and legal experts to discuss the state of play in preparing for cyberattacks and their mitigation, in Israel, the US and in the EU, aiming to inform the discussion on this timely topic.

**Roundtable: Security the ICT Supply Chain from Cybersecurity Threats**

* The Department of Homeland Security is embarking on an ambitious effort to advance our collective security through improved supply chain risk management action. By convening the IT and Communications sector coordinating councils and key government departments and agencies in a whole of government and industry initiative, the DHS ICT Supply Chain Task Force has a unique opportunity to advance focused solutions that align with the most serious threats.  This panel will feature the Task Force leaders who are tasked with achieving real-world results and will explore the many dimensions of supply chain security.

**Roundtable: Defending Operational Technology from Cybersecurity Threats**

* Exploitation of vulnerabilities in operational technology has the potential for significant national security and economic security impacts. As evidenced by the successful, temporary, disruptions to the functioning of Colonial Pipelines regional distribution system and the attack on the water facility in Oldsmar, Florida cyber adversaries are increasingly looking to impose cyber risk on operational technology networks. Defending these systems from malicious cyber actors requires a partnership between utilities, manufacturers, cybersecurity experts, and the public sector. Governments can amplify the threat and articulate the desire security and resilience outcomes, while enabling industry to innovate how to achieve real time visibility into operational technology threats, vulnerabilities, and risk.