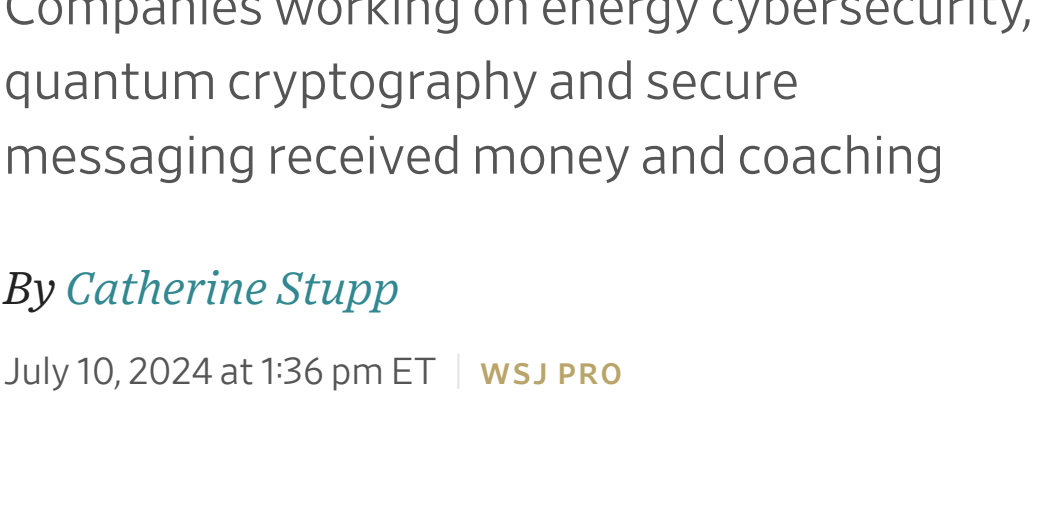
WSJ PRO

NATO Funds Startups Aiming to Solve Cyber Problems in Infrastructure

Companies working on energy cybersecurity, quantum cryptography and secure messaging received money and coaching

By Catherine Stupp

July 10, 2024 at 1:36 pm ET | WSJ PRO



NATO's Diana accelerator program funded 44 companies in its first cohort. PHOTO: JOHANNA GERON/REUTERS

The North Atlantic Treaty Organization is funding startups that build technology to protect critical infrastructure from cyberattacks.

The program, known as the Defence Innovation Accelerator for the North Atlantic, or Diana, launched late last year and marks the first time the military alliance has subsidized early-stage companies working on energy cybersecurity and secure communications systems.

"The mission is to locate and accelerate dual-use innovation across the alliance," said Tien Pham, chief scientist of the program, speaking during an event last month for the first cohort of startups. Dual-use goods can work for either civilian or military purposes.

Heads of state and government agencies are increasingly warning about cybersecurity threats to power grids and other critical infrastructure.

On Tuesday, the U.S. and seven allies warned of a Chinese state-sponsored hacking group threatening their networks. In June, the White House announced that the Group of Seven countries agreed to develop a cybersecurity framework for operational technologies to address the growing number of cyberattacks against energy systems.

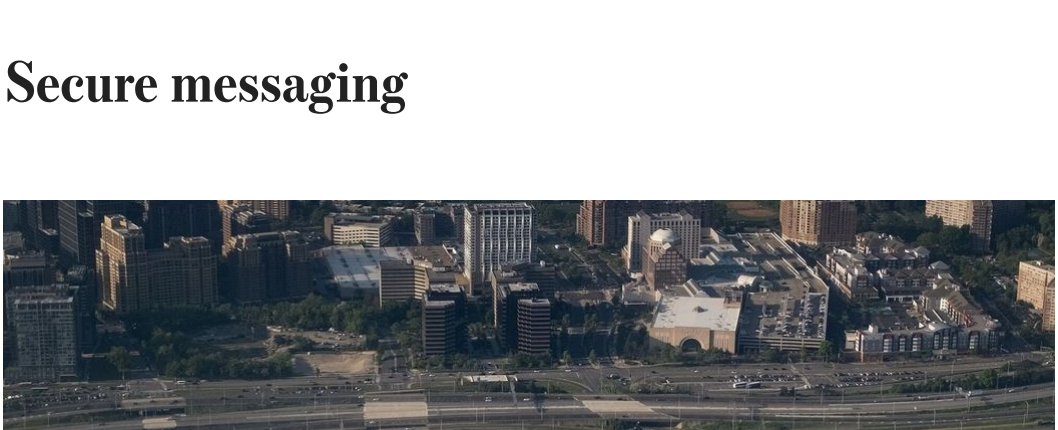
The 44 companies in Diana's first round were selected from 1,300 applicants in November and finished the six-month program in June.

In the first round, NATO gave each startup initial funding of 100,000 euros, equivalent to about $108,000, plus money for travel expenses. Extra funds are available to cover technology testing in a NATO-approved lab in Italy, Poland, Canada, the U.S. and other countries in the 32-nation alliance.

Startups selected to move on to the second phase of the program, scheduled to start this fall, will receive €300,000, plus additional coaching from scientists, engineers and others affiliated with Diana.

On July 1, the Diana project put out a call for a second cohort, focused on areas including energy, human health, information security, logistics and critical infrastructure.

Secure messaging


Militaries could use the Hushmesh secure-messaging app, CEO Manu Fontaine said. PHOTO: TOM BRENNER/BLOOMBERG NEWS

Hushmesh, in Falls Church, Va., is developing a secure-messaging application that could be used as an internal communications app for governments, militaries and businesses, said Chief Executive Manu Fontaine.

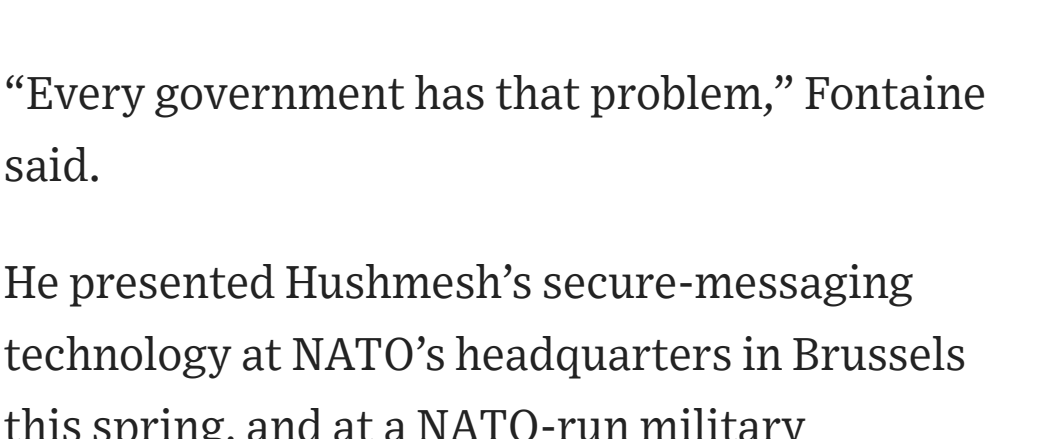
Fontaine, a Belgian living in the U.S., said the app runs on a network that doesn't rely on the domain name system that underpins the public internet. The startup's technology automates end-to-end cryptography to protect communication. The messaging app will have mobile and desktop versions and still allow government agencies and militaries to control the system, he said.

The U.S. military bans staff from using messaging apps and communication systems that aren't authorized by the Defense Department for official business. But in a report last year, the Pentagon's inspector general said military staff were violating that policy by using unauthorized commercial messaging apps on their work devices. The report recommended that the Pentagon require staff to forward all of their work messages on those apps to an official account.

"Every government has that problem," Fontaine said.

He presented Hushmesh's secure-messaging technology at NATO's headquarters in Brussels this spring, and at a NATO-run military communications tech conference. Introductions to military and government officials helped Hushmesh understand concerns about using existing commercial tools to communicate about sensitive topics, Fontaine said.

Infrastructure cybersecurity

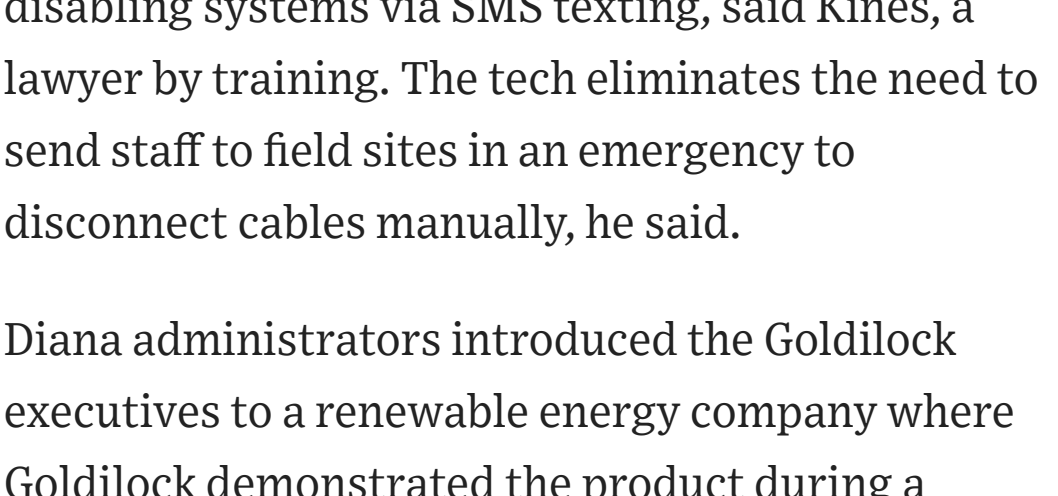

Goldilock is working on a remote kill switch to quickly shut down energy grids or other infrastructure. PHOTO: JORDAN VONDERHAAR/BLOOMBERG NEWS

Stephen Kines, co-founder and chief operating officer of U.K. startup Goldilock, is working on a remote kill switch for energy grids, water facilities and other infrastructure. The idea is to shut down systems quickly to stop a cyberattack from spreading.

Goldilock's device doesn't use the internet, instead disabling systems via SMS texting, said Kines, a lawyer by training. The tech eliminates the need to send staff to field sites in an emergency to disconnect cables manually, he said.

Diana administrators introduced the Goldilock executives to a renewable energy company where Goldilock demonstrated the product during a simulated cyberattack, Kines said.

Quantum cryptography


LevelQuantum aims to start testing its encryption terminals in the fall, CEO Magdalena Stobinska said. PHOTO: MICHAL LEPECKI/NCN

Milan-based LevelQuantum, another startup in Diana's first cohort, is developing encryption terminals based on quantum key distribution. The technology is more secure than today's cryptography because it can't be cracked by high-performance computers and quantum computers, said Magdalena Stobinska, chief executive.

Central banks, telecommunications carriers, and—since the startup participated in the Diana program—military agencies are interested in using the technology, she said.

LevelQuantum aims to start testing its product in the fall, to see if its software will connect people trying to communicate via a few quantum terminals, the way a bank with one terminal would connect its employees to a business partner with another terminal, Stobinska said.

Stobinska, a professor at the University of Warsaw in Poland, said the program introduced her to people in the military, helping her to understand their needs and concerns.

"It's not entirely clear where to start and how to talk, what are the steps and what are the red flags for them that you can raise unwittingly," she said.

Write to Catherine Stupp at catherine.stupp@wsj.com

BACK TO TOP