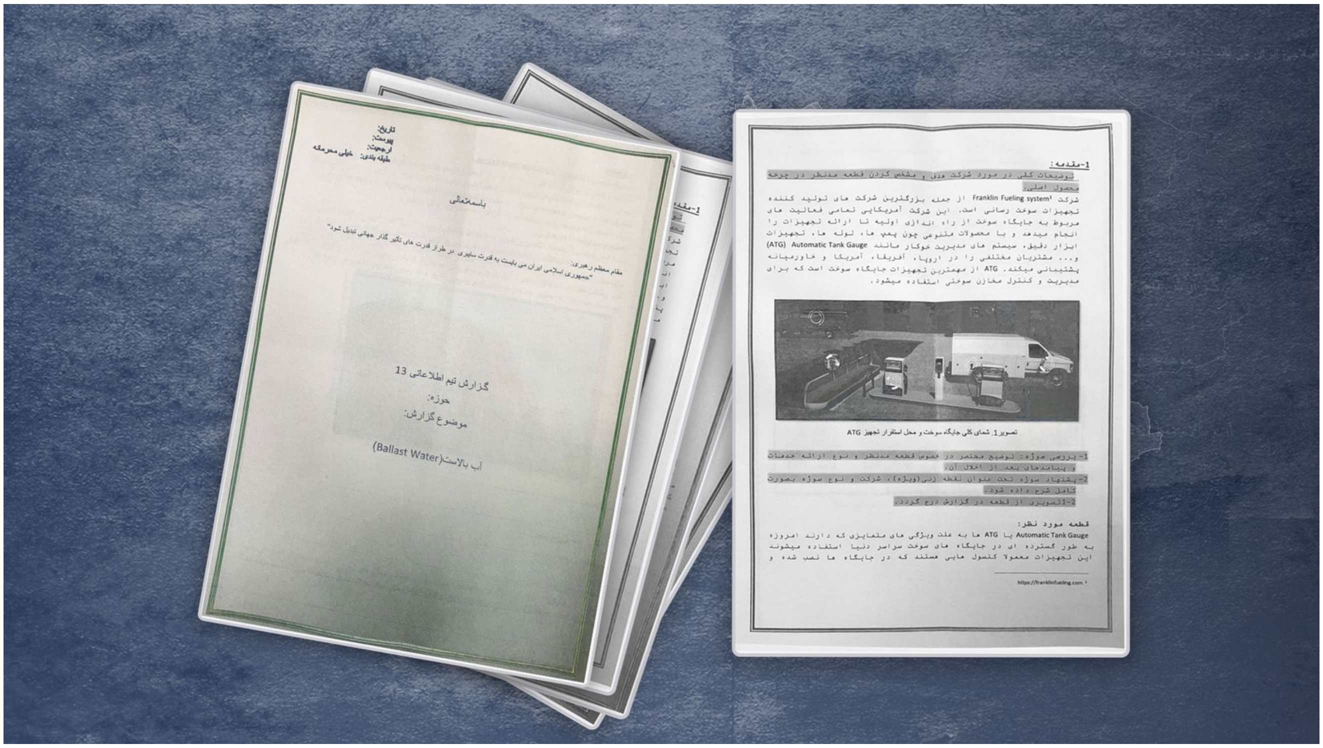
Iran's secret cyber files on how cargo ships and petrol stations could be attacked | World News

news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871

Sky



تاریخ:
پیوست:
ارجحیت:
طبقه بندی: خیلی محرمانه

باسمه‌تعالی

مقام معظم رهبری:
"جمهوری اسلامی ایران می بایست به قدرت سایبری در طراز قدرت های تاثیر گذار جهانی تبدیل شود"

گزارش تیم اطلاعاتی 13

حوزه:

موضوع گزارش:

آب بالاست(Ballast Water)

1-مقدمه:

توضیحات کلی در مورد شرکت هدف و مشخص کردن قطعه مدنظر در چرخه محصول اصلی.

شرکت Franklin Fueling system[1] از جمله بزرگترین شرکت های تولید کننده تجهیزات سوخت رسانی است. این شرکت آمریکایی تمامی فعالیت های مربوط به جایگاه سوخت از راه اندازی اولیه تا ارائه تجهیزات را انجام میدهد و با محصولات متنوعی چون پمپ ها، لوله ها، تجهیزات ابزار دقیق، سیستم های مدیریت خوکار مانند Automatic Tank Gauge (ATG) و... مشتریان مختلفی را در اروپا، آفریقا، آمریکا و خاورمیانه پشتیبانی میکند. ATG از مهمترین تجهیزات جایگاه سوخت است که برای مدیریت و کنترل مخازن سوختی استفاده میشود.

تصویر 1. شمای کلی جایگاه سوخت و محل استقرار تجهیز ATG

1- بررسی سوژه: توضیح مختصر در خصوص قطعه مدنظر و نوع ارائه خدمات و پیامدهای بعد از اخلال آن.

2- پیشنهاد سوژه تحت عنوان نقطه زنی(ویژه)، شرکت و نوع سوژه بصورت کامل شرح داده شود.

2-1تصویری از قطعه در گزارش درج گردد.

قطعه مورد نظر:

Automatic Tank Gauge یا ATG ها به علت ویژگی های متمایزی که دارند امروزه به طور گسترده ای در جایگاه های سوخت سراسر دنیا استفاده میشوند این تجهیزات معمولا کنسول هایی هستند که در جایگاه ها نصب شده و

[1] https://franklinfueling.com

تاریخ:
پیوست:
ارجحیت:
طبقه بندی: خیلی محرمانه

باسمه‌تعالی

مقام معظم رهبری:
"جمهوری اسلامی ایران می بایست به قدرت سایبری در طراز قدرت های تاثیر گذار جهانی تبدیل شود"

گزارش تیم اطلاعاتی 13

حوزه:

موضوع گزارش:

آب بالاست(Ballast Water)

By Deborah Haynes, foreign affairs editor

Classified documents, allegedly from Iran, reveal secret research into how a cyber attack could be used to sink a cargo ship or blow up a fuel pump at a petrol station.

The internal files, obtained by Sky News, also include information on satellite communication devices used by the global shipping industry as well as a computer-based system that controls things like lights, heating and ventilation in smart buildings across the world.

The papers appear to reveal a particular interest in researching companies and activities in western countries, including the UK, France and the United States.

A security source with knowledge of the 57-page bundle of five research reports said it was compiled by a secret, offensive cyber unit called Shahid Kaveh, which is part of Iran's elite Islamic Revolutionary Guard Corps' (IRGC) cyber command.

The source said he believed the work is evidence of efforts by Iran to collect intelligence on civilian infrastructure that could be used to identify targets for future cyber attacks.

"They are creating a target bank to be used whenever they see fit," said the source, who requested anonymity to be able to talk about the documents.

The Iranian embassy in London did not respond to a request for comment on the allegations.

A growing number of countries, including the UK, possess cyber weapons and are working to develop new offensive capabilities.

The work is typically top secret.

So it is highly unusual to see documented evidence allegedly of cyber research by a state.

[redacted]

INSIDE THE DOCUMENTS

Each of the five reports are marked 'very confidential'.

Towards the top of most of the files is a quote, which appears to be from Iran's Supreme Leader, Ali Khamenei. It reads: "The Islamic Republic of Iran must become among the world's most powerful in the area of cyber." The security source describes the quote as like a "commander's statement of intent".

The reports are compiled by a cell called Intelligence Team 13. The source with knowledge of the files refers to them as Intelligence Group 13 and said it is a sub-group within the IRGC Shahid Kaveh unit, under an individual he named as Hamid Reza Lashgarian.

"They are supposed to be rather clandestine. They work on offensive cyber operations globally," the source said.

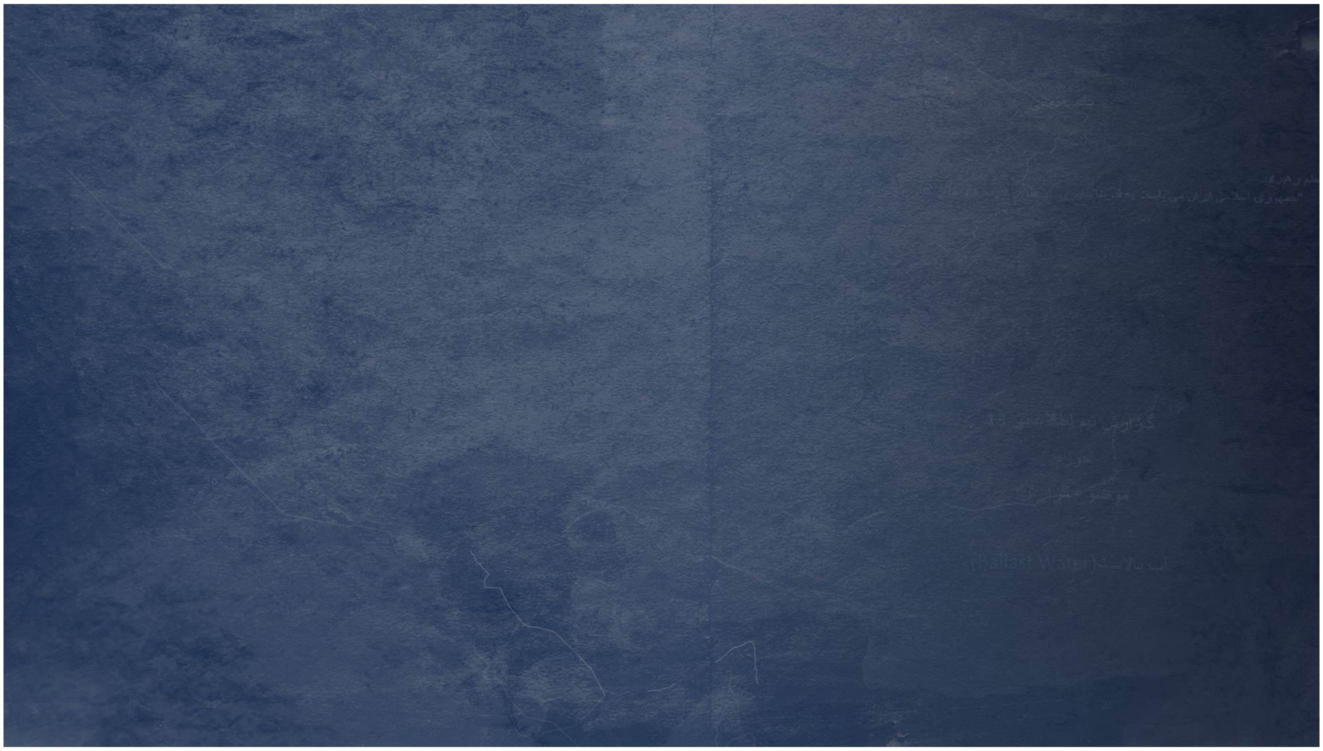
Only two of the reports have a completion date on their front page.

One, which looks at what is known as a building management system – the computer technology that controls things like lights, heating and ventilation in smart buildings – is from 19 November 2020.

Another, which looks at a German company called WAGO that manufactures electrical components, is dated 19 April 2020.

Two of the other reports, one into fuel pumps at petrol stations and another into maritime communications, include screen shots of internet searches dated to last year.

[redacted]


گزارش تیم اطلاعاتی 13
آب بالاست(Ballast Water)

BALLAST WATER

One of the reports was entitled "Ballast Water". Across six pages, it looked at the complex systems on large cargo ships that control things remotely like filtration and ballast water. The authors appeared to rely on open source research rather than any privileged information.

A diagram illustrated a ship steady in the water, while another one showed a ship tilted to one side. A caption underneath it said: "Picture three off balance".

Another diagram showed how commands could be sent remotely to a ship from a control centre on land via a satellite link.

The report said: "These pumps are used to bring water into the tanks through centrifuges and in order to operate correctly, the task must be completed with precision. Any problems could result in the sinking of the ship."

In a concluding note, it observed: "Any kind of disruptive influence can cause disorder within these systems and can cause significant and irreparable damage to the vessel."

[redacted]

FUEL PUMPS

Another piece of research was into a system called an automatic tank gauge that tracked the flow of fuel at a petrol station. The report, which was also six pages long, name-checked fuelling equipment produced by Franklin Fueling Systems, a US company.

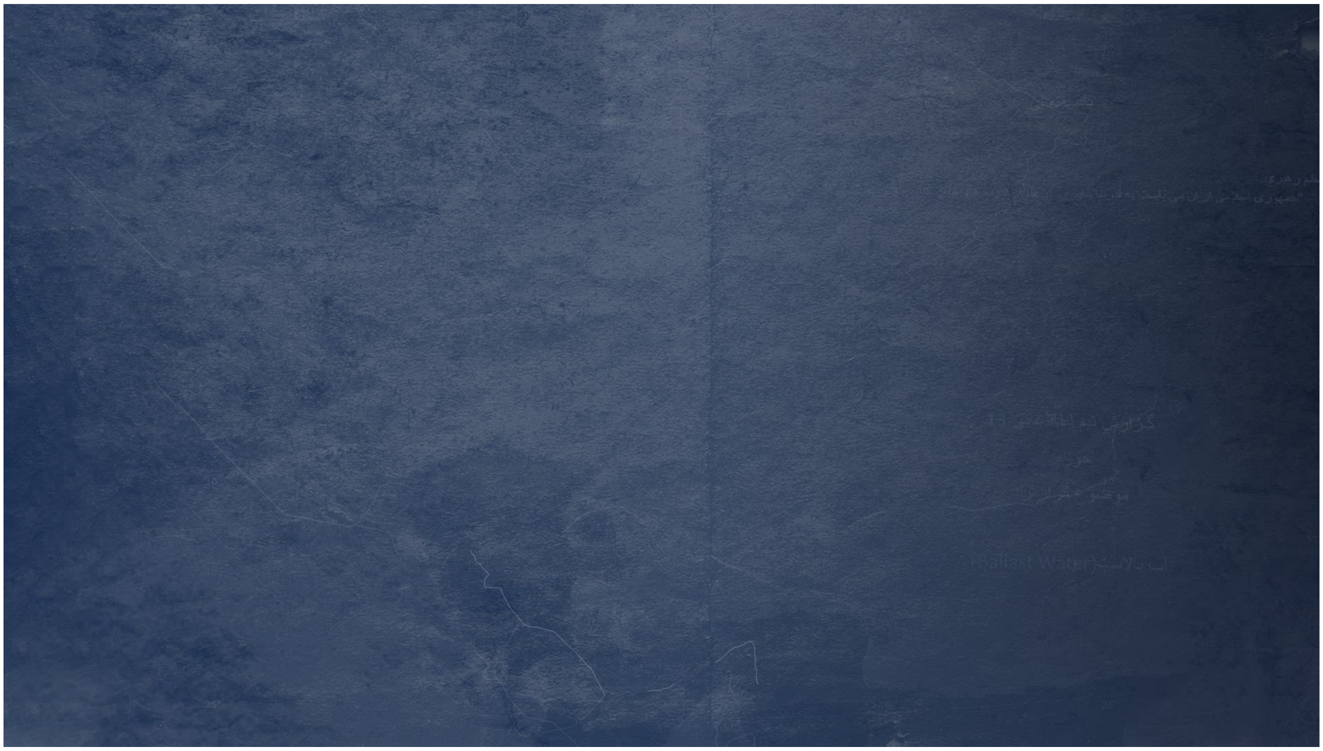
"They support many customers in Europe, Africa, America and the Middle East and they can control and manage these systems," it said.

Illustrated with a photograph of a petrol station and an image lifted from the website of Franklin Fueling Systems, the file spelt out what it believed would be the impact of a "problem" with the systems.

This includes the ability to cut off the fuel supply or change its temperature.

The report added: "[An] explosion of these fueling pumps is possible if these systems are hacked and controlled remotely."

[redacted]

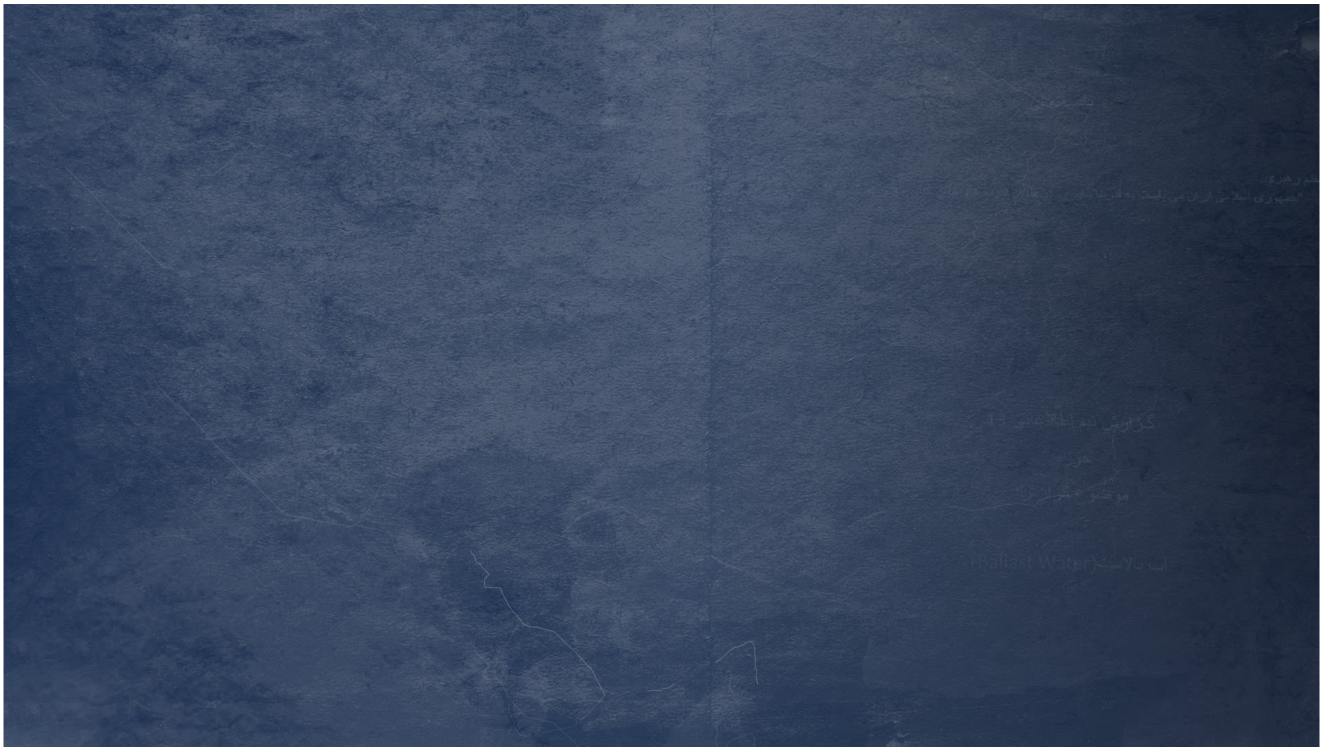


A spokesman for Franklin Fueling Systems said the company takes "seriously the need to provide highly reliable and secure equipment to our customers".

He said it could be possible for a third party to cause issues with one or more petrol stations. But he said he did not think it would be possible to trigger an explosion.

"There are a number of redundant safety systems involved in a typical fueling station, and we do not believe that an explosion could be caused through control of the automatic tank gauge or fuel management system, even if that were the user's intent," the spokesman said.

[redacted]



MARITIME COMMUNICATIONS

This report, 14 pages long, looked at two types of satellite communication used at sea.

One, called Seagull 5000i, provides phone, fax and other data services via a satellite link. The report noted that it is a service offered via companies such as Wideye in Singapore and Thuraya in the United Arab Emirates.

The other system of interest is called Sealink CIR.

Most of this file was simply open source research repeating facts about two systems.

But there was also a chart towards the end of the file that showed the results of what is known as a "Google dork" – conducting internet searches with certain key phrases enclosed in quotation marks to improve the accuracy of the search.

The authors of the report used the Chinese search engine Fofa.so as well as Binaryedge, a search engine for internet-exposed devices, which is owned by a US company to search for Seagull 5000i and Thuraya in the United States, the United Kingdom, France, Israel and a number of other countries.

One column listed a percentage figure, another listed the number of devices.

Sarah Jones from cyber security firm FireEye's Mandiant Threat Intelligence unit, who has analysed the files, said it could refer to the percentage of devices whose log-in screens can be seen from the internet search.

The document included a screen shot of a log-in screen. But there was no evidence that the researchers went beyond conducting the search, such as attempting to access accounts.

[redacted]

SMART BUILDINGS

The other two reports were the only two that include a formal date on the front for when they were compiled.

The most recent was one into building management systems – the computer-based systems that control lighting, ventilation, heating, security alarms and other functions in a smart building. Nine pages long, it was dated the Iranian calendar's equivalent of 19 November 2020.

The documents listed companies that provide these services. They included Honeywell in the United States; the French electrical equipment group Schneider Electric; the German giant Siemens; and KMC Controls, another US manufacturer.

The longest report – 22 pages – was into electrical equipment made by the German company WAGO. It was dated the Iranian calendar’s equivalent of 19 April 2020.

The file examined vulnerabilities in what is called a programmable logic controller or PLC – a computer control system.

But the authors appeared to conclude that it would not be possible to exploit them.

"Continuing the investigation, in order to use these processes, we noticed the vulnerabilities within these systems are irreparable, if there is an attack, damage will not easy to fix," the report said.

"Therefore, compared to other PLC brands, this brand is impenetrable once connected online. When online, the infrastructure and intelligence on engineering cannot be reached and cannot be lost.

"For our benefit, the best situation is for the PLC not to work as intended, and for that to happen, a project must be written in the language of ladder to have multiple exits, as many as possible. But the problem for this project is that we wouldn’t be able to assess the damage caused. The other option is to assess the weak points and dangerous points of the PLCs and software in order to attack our target. This option needs separate investigation and research before we can find the weak points."

A THREAT TO 'OUR WAY OF LIFE'

Ben Wallace, Britain's defence secretary, said the Iranian documents – if authentic – demonstrate how vulnerable the UK and its allies are to cyber attacks.

"Unless we do something about it, our critical national infrastructure, our way of life could be threatened quite easily," he told Sky News.

[redacted]

Asked how much of a threat Iran poses in cyber space, General Sir Patrick Sanders, the top military officer overseeing UK cyber operations, said: "They are among the most advanced cyber actors. We take their capabilities seriously. We don’t overstate it. They are a serious actor and they have behaved really irresponsibly in the past."

The source who shared the Iranian documents with Sky News said he was "very confident" they were authentic.

Sky News shared the files with additional sources that would have the ability to tell if they seemed authentic.

These sources indicated that they thought the files looked credible and interesting.

Sky News also shared the cache with the US cyber security company FireEye, which investigates the Iranian cyber threat as well as those from other hostile states.

Mandiant Threat Intelligence, a part of FireEye, said: "The documents seem to emphasise simple, opportunistic attacks.

"They discuss the possible physical impacts of cyber operations targeting civilian critical infrastructure and the feasibility of conducting such attacks, while examining the percentage of internet-accessible devices that could be potential targets."

It said that the five reports, which comprise the bundle, appear to be a response to a request for information or research.

"Everything that was outlined in the documents really fits in with what we have seen from Iranian capabilities and the way they plan their attacks, the way they structure and divide up the work and go out and actually start the process of forming an operation," said Sarah Jones, senior principle analyst at Mandiant.

She said these are the initial steps a state would take if they wanted to develop a specific cyber attack capability.

"You are seeing all of that set up but you are not seeing any of the other phases of that. You are seeing them saying – what would happen if we were to do this and how could someone go about causing some sort of damage or destructive capabilities to really a lot of different technologies?" she added.

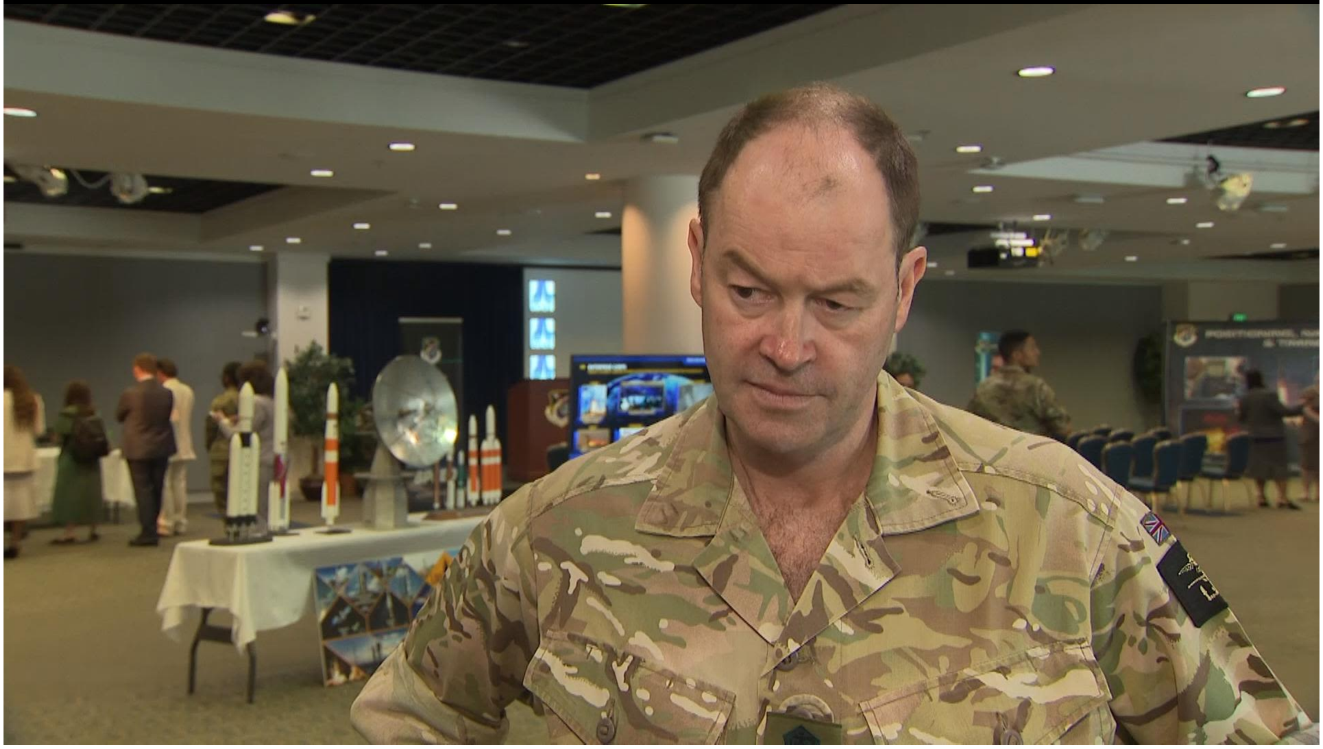
WHY IT MATTERS

Iran is not the only country seeking to develop new methods of attack in cyber space.

The UK and its allies, as well as adversaries such as Russia, China and North Korea, are all investing heavily in building new offensive capabilities.

The difference, according to British officials, is the targets that hostile states are willing to go after in peacetime - from attempting to manipulate elections to causing physical damage to civilian infrastructure like water supplies and petrol pumps.

"I think it is perfectly legitimate for states to seek to enhance their capabilities to defend and protect themselves in cyber space," General Sir Patrick Sanders, commander of the UK military's Strategic Command, which overseas British cyber operations, told Sky News.



"There is nothing wrong with that. But if you are using them in ways that are malign and irresponsible you can cause harm or economic damage then that's not acceptable."

Cyber is an area where countries can covertly harm each other, steal secrets or manipulate minds without fear of triggering a more conventional war – though a sufficiently devastating attack from cyberspace could have that effect.

The UK does have the ability to cause harm in the same way as its opponents – but says it is a power only used to counter a threat or respond to an attack.

Any cyber operation must be "responsible, targeted and proportionate", according to rules governing the UK's National Cyber Force, which is a partnership between the military and the spy agency GCHQ.

By contrast, Iranian-linked hackers are suspected of targeting the UK parliament in 2017, with thousands of email accounts, including those of MPs, affected.

While Iran is viewed as a cyber threat, the country has also been the victim of multiple cyber attacks – many of them targeted against its nuclear programme.

One of the first-known offensive cyber attacks was the Stuxnet virus, allegedly developed by Israeli and US cyber spies, that was discovered at a uranium enrichment facility at Natanz in 2010.

More recently, in May last year computers at Iran's Shahid Rajee port terminal crashed, bringing traffic to a halt, following a cyber attack that reportedly originated from Israel.

It was allegedly in retaliation to an Iranian attempt to hack Israel's water systems – an act that prompted Yigal Unna, Israel's national cyber chief to warn that "cyber winter is coming".

It should come as little surprise that Iran appears to be gathering information to hone its offensive cyber capabilities.

China and Russia are viewed by the UK as the most potent, hostile cyber threats, followed by Iran and North Korea.

But Britain and some of its allies, in particular the United States and Israel, also have the ability to launch attacks in cyberspace.

They just operate under different rules of engagement.

With so much of the world reliant on the internet, computers and access to information, cyber is a growing domain of conflict, where nations, criminals and lone hackers are able to inflict damage or help in their side's defence.

Cyber attacks typically happen in a grey zone of harm that lies between war and peace.

Sky News produced a podcast series on this evolution in the nature of warfare.

In the grey zone, anything can and is being weaponised, from spreading malware on a computer or publishing fake news to poisoning an opponent or bribing a politician.

It means the act of leaking information also plays a part in this contest.

And no one is too unimportant to be a target.

Credits:

Reporting: Deborah Haynes, foreign affairs editor

Production: Leo Lord Jones, foreign affairs producer

Design: Brian Gillingham and Arianne Cantwell

[redacted]

Top