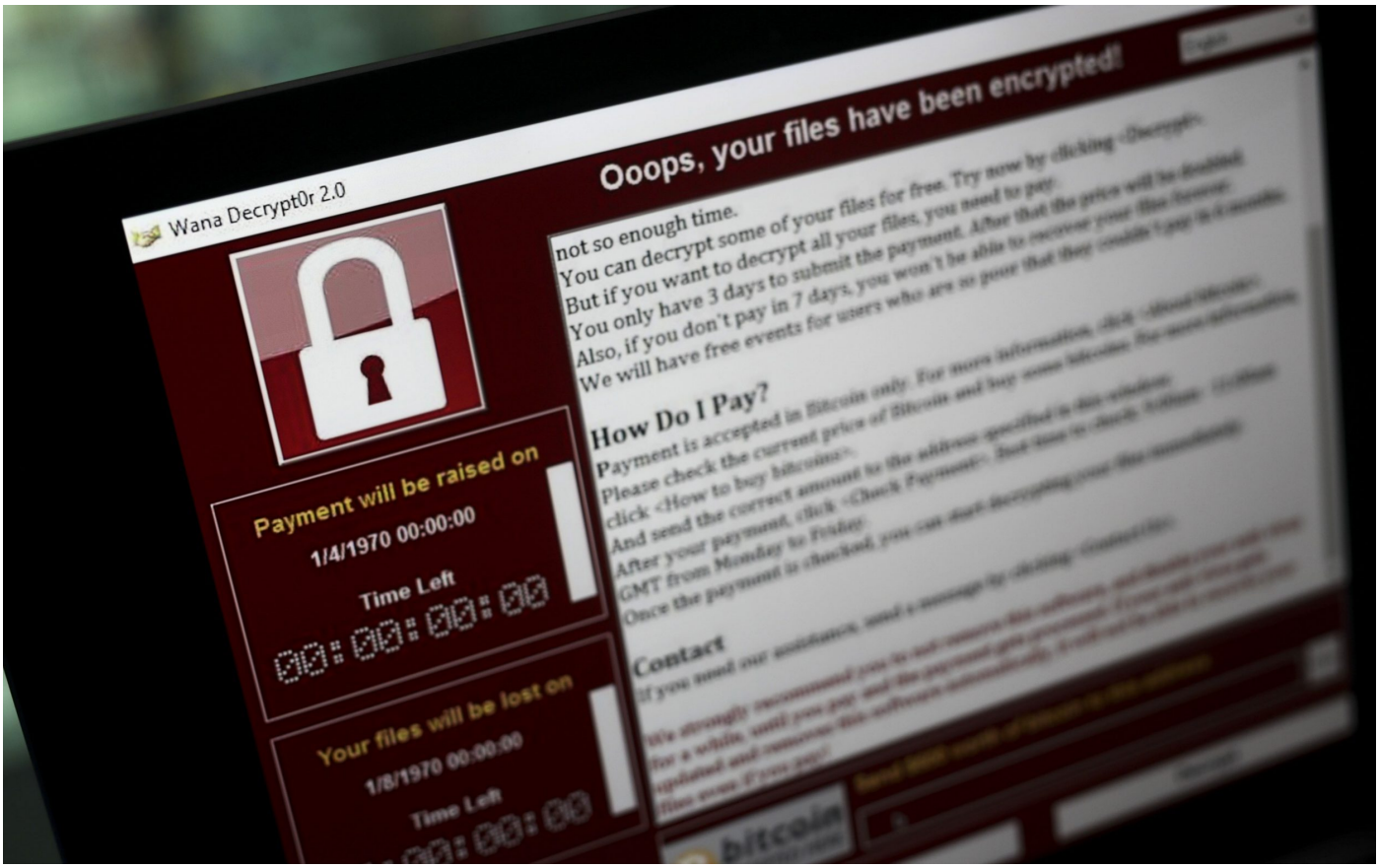
EU governments to warn cyber attacks can be an act of war



A lock screen from a cyber attack warns that data files have been encrypted CREDIT: SIMON DAWSON/BLOOMBERG

By **James Crisp**, BRUSSELS CORRESPONDENT

29 OCTOBER 2017 • 9:17PM

European Union governments will formally state that cyber attacks can be an act of war in a show of strength to countries such as Russia and North Korea.

Diplomats and ambassadors in Brussels have drafted a document, obtained by The Telegraph, that represents an unprecedented deterrent aimed at countries using hackers and cyber espionage against EU members.

The document, set to be agreed by all 28 EU members states, including Britain, in the coming weeks warns that individual member states could respond "in grave instances" to cyber attacks with conventional weapons.

The British government (http://www.telegraph.co.uk/news/2017/06/24/parliament-hit-sustained-determined-cyber-attack/) has now said it was all but certain that North Korea was behind the "WannaCry" (http://www.telegraph.co.uk/science/2017/10/27/home-office-blames-north-korea-devastating-nhs-wannacry-cyber/)malware attack that hit NHS IT systems in May. Work on the EU paper began among fears that Russia would attempt to influence this year's German elections and over hybrid warfare employed in Ukraine (http://www.telegraph.co.uk/news/2017/09/04/people-going-die-latvias-foreign-minister-warns-covert-cyber/).

About | WannaCry

What is it?
Also known as Wanna Decryptor or wcry, it is a piece of malicious software that encrypts files on a user's computer, blocking them from view and threatening to delete them unless a payment is made.

How is it installed?
The virus made it onto computers thanks to a vulnerability in Windows that was exploited using a tool named EternalBlue, believed to be first developed by America's NSA. Many computers had not been updated with protection against the exploit.

What does it do?
Once opened, the virus is able to encrypt files and block user access to them, displaying a pop-up window on-screen telling users they have been blocked and demanding payment - often via a digital currency such as Bitcoin.

Can you remove it without paying?
Yes, by using advanced anti-malware software. The malware can also be removed manually with a computer in "safe mode", however security experts warn this runs the risk of damage to a PC as users must go through sensitive system files in order to find and isolate files created by the Wanna Decryptor software.

Source: PA

The Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities states that a country under attack can exercise its "inherent right of individual or collective self-defence" under international law.

"The EU is concerned by the increased ability and willingness of state and non-state actors to pursue their objectives by undertaking malicious cyber activities," the paper reads.

In a clear signal of governments' desire to send a strong message, the document explicitly states that a member state can invoke the EU's mutual defence clause.

Article 42 (7) of the EU Treaty allows a member state to demand "aid and assistance" from its fellow EU governments. "If a member state is the victim of armed aggression on its territory," the article states, "the other member states shall have towards it an obligation of aid and assistance by all the means in their power."

This would trigger bilateral discussions and potential alliances between EU countries, which could go beyond the constraints of common EU foreign policy. The limits of what "aid and assistance" could represent is vague and is purposefully left up to individual governments to decide between themselves.

The mutual defence clause was invoked for the first and only time by France after the Paris terror attacks in 2015. EU defence ministers agreed unanimously to provide France with military assistance.

The EU itself cannot wage war but the paper warns it could provide support to any member state or coalition of member states reacting lawfully to a cyberattack. Such responses can range from diplomatic steps to "the use of stronger individual or cooperative responses."

EU support to such action can range from public condemnation, diplomatic pressure and sanctions, including economic measures, arms embargoes and travel bans.

"This will make an attacker weigh the consequences of a cyber attack more carefully," said one EU source, "and setting out the steps in a formal document shows we are serious."

The EU move comes after NATO said in June that an Article 5 response (http://www.telegraph.co.uk/news/2017/06/28/nato-assisting-ukrainian-cyber-defences-ransom-ware-attack-cripples/) was possible if a cyber attack met the international legal definition of an act of war.

Article 5 obliges NATO countries to treat an attack on one member as an attack on all members. Most but not all EU member states are members of NATO.

WannaCry ransomware map
Locations of infection