The IPT ruled that GCHQ spies can legally hack any electronic devices

February 13, 2016 By Pierluigi Paganini

The British Intelligence Agency GCHQ has a license to hack computers and devices, the UK's Investigatory Powers Tribunal (IPT) ruled.

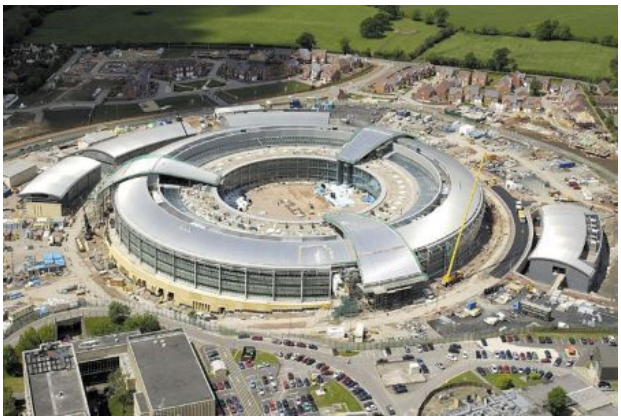
This means that the UK Government is giving full power to its intelligence agency to spy on Britons as well as people living abroad.

The verdict was issued on Friday after Privacy International and seven ISPs launched a legal challenge against the conduct of the CGHQ whom hacking operations were revealed by documents leaked by NSA whistleblower Edward Snowden.

The CGHQ is responsible of "persistent" illegal hacking of electronic devices and networks worldwide, the Investigatory Powers Tribunal (IPT) has been told.

The popular whistleblower Edward

revealed the existence of secret surveillance activities such as the Tempora operation and hacking platforms such as the Smurf suite.



GCHQ admitted for the first time that government monitoring station in Cheltenham carries out "persistent" and "non-persistent" Computer Network Exploitation (CNE) against targets in the UK and abroad.

In 2013, the tribunal was told, 20% of GCHQ's intelligence reports contained information that was obtained through hacking operations.

The case has been brought in hearing at the IPT which deals with complaints against the surveillance operated by the UK intelligence. A four-day hearing is at the Rolls Building in central London.

"The [legal] regime governing CNE … remains disproportionate," Ben Jaffey, counsel for Privacy International, told the tribunal. "Given the high potential level of intrusiveness, including over large numbers of innocent persons, there are inadequate safeguards and limitations."

Jaffey highlighted that GCHQ's hacking alter the targeted systems, an activity that is not considered legal by the authorities.

"The use of computer network exploitation by GCHQ, now avowed, has obviously raised a number of serious questions, which we have done our best to resolve in this Judgment," reads the lengthy ruling from the Investigatory Powers Tribunal (IPT).

"Plainly it again emphasises *the requirement for a balance to be drawn between the urgent need* of *the*

Intelligence Agencies to safeguard the public and the protection of an individual's privacy and/or freedom of expression."

The court has investigated the legality of the methods used by British intelligence

The tribunal investigated "investigates and determines complaints of unlawful use of covert techniques by public authorities infringing our right to privacy."

In some cases, the GCHQ installed malware on targeted systems and hacked mobile devices with its Smurf suite.

In November 2015, for the first time the technological abilities of the UK's National Crime Agency (NCA) have been revealed in a collection of documents, the British law enforcement agency has "equipment Interference" (EI) capabilities, which allow it to hack into mobile devices and computers.

Eric King, the deputy director of the Privacy International, who analyzed the document noticed that in a section there is the explicit reference to the capability of the UK law enforcement having the capability to conduct "equipment interference."

"Equipment interference is currently used by law enforcement agencies and the security and intelligence agencies," states the section. The documents also reveal that "more sensitive and intrusive techniques" are available to a "small number of law enforcement agencies, including the National Crime Agency."

> "
>
> UK law enforcement a in hacking business according to IP Bill pic.twitter.com/SAGz
>
> — Eric King (@e3i5) November 2015

The GCHQ hacking operations were conducted

under a self-imposed code of conduct, the IPT recognizes as legal these activities despite the chagrin of privacy advocates.

"We are disappointed that the IPT has not upheld our complaint and we will be challenging its findings," said Scarlet Kim, legal officer at Privacy International.

I wonder at this point what will be the repercussions of such a decision on the international level. This decision authorizes in fact any government to hack systems of foreign states. We are in the far west.

Pierluigi Paganini

(Security Affairs – GCHQ, hacking)

Share it please ...

CGHQ | equipment interference | Hacking | IPT | NSA | surveillance | UK

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency

for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

PREVIOUS ARTICLE

BlackEnergy infected also Ukrainian Mining and Railway Systems

NEXT ARTICLE

Iranian hackers compromised former IDF chief's computer

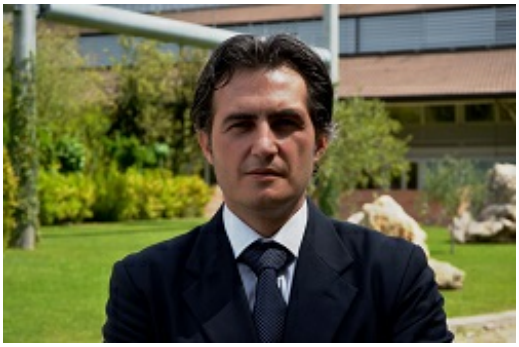
YOU MIGHT ALSO LIKE

Man charged of Laundering $19.6 Million earned with PBX system hacking

February 14, 2016 By Pierluigi Paganini

BlackEnergy infected also Ukrainian Mining and Railway Systems

February 13, 2016 By Pierluigi Paganini



- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

1. Best Antivirus Software 

2. Remove Antivirus Scan 

3. Cheap Laptops Online 

4. Cell Phone Reviews 

5. Top 10 Cell Phones 

6. Password Management Software 

7. Computer Repair Services 

8. Protect Your Privacy 

Back to top