PHYS.ORG

Increased fragmentation of 'dark Web' poses great security challenge

February 19 2015

It would not be surprising to see the dark Web's criminal underbelly become more fragmented, and therefore more complicated to investigate given wide-spread online surveillance by states and the recent arrests of cybercriminals. This is according to a new working paper issued by the Global Commission on Internet Governance (GCIG).

The Impact of the Dark Web on Internet Governance and Cyber Security is authored by former US Homeland Security Secretary Michael Chertoff and Tobby Simon, president of the India-based Synergia Foundation.

The new report was recently presented at the GCIG meeting that took place from February 14-15 in London, United Kingdom. The GCIG is a two-year initiative launched by the Centre for International Governance Innovation (CIGI) and Chatham House. Chaired by former Swedish Prime Minister Carl Bildt, the commission will produce a comprehensive stand on the future of multi-stakeholder Internet governance.

In the new report, Chertoff and Simon say "in order to formulate comprehensive strategies and policies for governing the Internet, it is important to consider insights on its farthest reaches—the deep Web and, more importantly, the dark Web."

The authors acknowledge that "anonymous communications have an important place in our political and social discourse…due to concerns about political or economic retribution." But the dark Web, a subset of the massive deep Web, has allowed for anonymous cybercriminals to take part in a range illegal activity. As an example, the authors point out that "the dark Web and terrorists seem to complement each other—the latter need an anonymous network that is readily available yet generally inaccessible."

"While the dark Web may lack the broad appeal that is available on the surface Web, the hidden ecosystem is conducive for propaganda, recruitment, financing and planning, which relates to our original understanding of the dark Web as an unregulated space," the authors say.

"Providing evidence showing that the dark Web has turned into a major platform for global terrorism and criminal activities is crucial in order for the necessary tools to be developed for monitoring all parts of the Internet," according to Chertoff and Simon. They recommend the following efforts to monitor the dark Web:

- mapping the hidden services directory by deploying nodes in the DHT;
- customer data monitoring by looking for connections to non-standard domains;
- social site monitoring to spot message exchanges containing new Dark Web domains;
- hidden service monitoring of new sites for ongoing or later analysis;
- semantic analysis to track future illegal activities and malicious actors;
- marketplace profiling to gather information about sellers, users and the kinds of good exchanged.

More information: The report is available online: www.cigionline.org/sites/defau … s/gcig_paper_no6.pdf

Provided by Global Commission on Internet Governance

Citation: Increased fragmentation of 'dark Web' poses great security challenge (2015, February 19) retrieved 27 April 2024 from https://phys.org/news/2015-02-fragmentation-dark-web-poses-great.html