|  |  |
| --- | --- |
| **COUNCIL WORKING GROUP ON CHILD ONLINE PROTECTION** 17th meeting, Virtual meeting, 26 January 2021 |  |
|  |  |
|  |  |
|  | **Document CWG-COP-17/4-E** |
| **12 January 2021** |
| **English only** |

**CONTRIBUTION FROM THE RUSSIAN FEDERATION**

**CHALLENGES GENERATED BY USING ENCRYPTION PROTOCOLS ON THE INTERNET ENABLING CONCEALMENT OF NAME (IDENTIFIER) OF AN INTERNET RESOURCE**

1. **Introduction**

The development of technologies, services and business on the Internet leads new challenges to personality, society and state.

Currently, encryption methods enabling the concealment of the name (identifier) of Internet resources are developed and implemented in software products. The creation and usage of such encryption methods are displayed as enhancement of security for users by preventing the interception and manipulation of DNS queries, and of anonymity and security of user data. It is quite clear why such solutions are developed. Given that DNS UDP has hardly changed since the early 1980's, and back then it was developed without any security considerations, while up-to-date IT tools and possibilities of hackers have substantially improved, the problem of using DNS services "as it is" has become even more urgent and in many cases it poses a serious danger both to business and private users. Types of DNS attacks existing today can lead not only to the leakage of financial information (both individuals and companies) or trade secret, but to stealing of the finances themselves, both clearly and literally (for example, by spoofing network packets in remote banking system) and implicitly (trade secret and competitors).

According to expert estimation, there is an increase in the number of cases when masking protocols, enabling the concealment of actual network addresses of devices from external systems and encryption protocols, are used. Protocols with cryptographic algorithms and ESNI, DoH (DNS over HTTPS) and DoT (DNS over TLS) encryption methods are becoming even more widely-spread.

At the same time, when implementing such encryption methods, the issue of assuring public interests, particularly, child online protection remains unclear. Implementation of these encryption algorithms and methods can decrease the usage efficiency of current illegal content filtering systems and child online protection systems.

Generally, risks and threats to the encryption implementation can include:

* a difficulty to block sites containing illegal and harmful content by efforts of system administrators and providers;
* an impossibility for common users to configure parental control on browsers;
* an impossibility to track and counteract malware (if computer is infected) by analyzing its network behavior;
* a difficulty in organizing a national Law Enforcement Support System in the national cyberspace;
* an actual rejection from DNS-inherent decentralization in favour of utilization of a DNS resolver with encryption; DNS traffic reallocation and a threat of “privatization” of the critical Internet infrastructure by major players which have vertically-integrated digital ecosystems;
* a concentration of potentially sensitive user data at operators of DNS resolvers with encryption (if their number will be limited and they'll serve as points of attraction).

Russian Federation has repeatedly expressed concern about these challenges at international platforms to arrange the uttermost full-scale discussion of the necessity to respect public interest, specifically, child online protection, while involving other states, IGOs, and INGO in cooperation and support of the Russian position for consolidated activity on this issue.

1. **Proposal**

Russian administration would like to express its support to the studies aimed at the development of advanced technologies applicable on the Internet; however, we also express concern about the question: how public interest would be considered for managing the child online protection during implementation of these technologies, particularly, encryption protocols enabling the concealment of name (identifier) of an Internet resource?

We propose to arrange discussion of issues related to implementation of ESNI, DoH (DNS over HTTPS), DoT (DNS over TLS) Internet encryption protocols enabling the concealment of name (identifier) of Internet resource in CWG-COP under the following general plan:

1. To suggest governmental representatives to discuss the issues related to child online protection under the implementation of ESNI, DoH (DNS over HTTPS), DoT (DNS over TLS) Internet encryption protocols with national child welfare authorities and organization, national law enforcement authorities, and all stakeholders at the national level, and to give their views at the next CWG-COP meeting for further discussion.
2. To request ITU-T SG 17 to share their views with CWG-COP regarding child online protection under the implementation of Internet encryption protocols enabling the concealment of the name (identifier) of an Internet resource.
3. To forward a proposal to the ITU Council requesting to instruct CWG-Internet to consider challenges on ensuring public interest during the implementation of Internet encryption protocols enabling the concealment of the name (identifier) of an Internet resource, and public policy issues on that subject, and also to submit the results to CWG-COP.
4. Based on the deliverables obtained, to arrange a wide discussion in CWG-COP, involving Member States and stakeholders, and develop, if required, recommendations on child online protection under the implementation of Internet encryption protocols enabling the concealment of the name (identifier) of an Internet resource for future consideration by the ITU Council.

\_\_\_\_\_\_\_\_\_\_\_