How the Internet amplifies threats to society and what to do about it

Discussion item for Ethical Forum
University Foundation, Brussels
Dec. 7, 2017

Peter Van Roy
Université catholique de Louvain

Today's Internet technologies greatly exacerbate threats to the healthy functioning of a democratic society. They enormously amplify the problems of alternative facts, i.e., false information, and echo chambers, i.e., where one only hears what one agrees with. The ease and rapidity with which any individual can disseminate their opinions and connect with others have never been greater, with the enormous success of social networks such as Facebook, micromessaging tools such as Twitter, and blogging software that allows anyone to publish anything. In the 1970s, the Internet was conceived by a community of idealists, who believed that an open and trusting environment would be to the benefit of everyone. Now we realize that this ideal was not realistic; that today many groups use the Internet as a terrain on which to battle ruthlessly to advance their own goals.

Organized misuse of the Internet takes many forms. Misinformation sites such as InfoWars continuously spout conspiracy theories and slander. Propaganda organizations engage in online influence campaigns using social networks. The ironically named Internet Research Agency is funded by the Russian government to undertake massive trolling campaigns and has successfully influenced the 2016 US presidential election and the UK Brexit referendum. Botnets (Mirai, Reaper, and many more) hijack large numbers of Internet-connected devices for DDoS (Distributed Denial of Service) attacks. Criminal organizations exploit security flaws to endanger citizens' private lives (identity theft, ransomware, theft of credit card numbers and medical histories, etc.). All these approaches are efficient precisely because the Internet was not originally designed to thwart them.

Internet technologies must urgently be updated to address these and other misuses. The foundation of a hypothetical new “protected Internet” is clearly strong cryptographic security, which is easily usable by all and unbreakable even for powerful organizations. However, that is only the first step. We urgently need to change the way that Internet collaboration works. For example, all email should be encrypted (most emails are still sent in cleartext), all news items should be digitally signed with provenance information (which defines the origin of the news), and user identities should be traceable to physical persons so that social networks can require physical identity if so desired. Sensitive information should be managed by its owner, instead of dispersed over large Internet companies (such as GAFA). Some progress has been made, for example many Web sites now use the https protocol, which is a secure version of the http protocol that was designed to enable Web commerce. But this is by far not enough. We need to take urgent action to turn the tide.

Academic communities, in particular universities, can be pioneers in the effort to make a protected Internet by themselves adopting updated technologies and thus setting the example for others. Reputable sources of information can then follow and adopt these technologies as well. Readers will be able to verify that an article comes from the New York Times instead of from InfoWars. Social networks will be able to verify that a user is a physical person in Europe and not a Russian troll. Thus, we hope that the open Internet and its misuses will be relegated to a temporary period in Internet history.