FUNDACJA PANOPTYKON

Warszawa, 23 października 2012 r.

Szanowny Pan
Michał Boni
Minister Administracji i Cyfryzacji

Szanowny Panie Ministrze,

Fundacja Panoptykon dziękuje za zaproszenie do przedstawiania uwag do projektu Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej (dalej: Polityka, projekt). Na wstępie chcemy zaznaczyć, że doceniamy fakt przygotowania kompleksowego podejścia do problematyki cyberprzestępczości, a także włączenia organizacji społecznych w proces jej tworzenia. Ogólny poziom projektu nie pozwala nam jednak na przedstawienie szczegółowych uwag – mamy nadzieję, że będziemy mieli tę możliwość na etapie wdrożenia Polityki, w szczególności jeśli będzie to za sobą pociągało jakiekolwiek prace legislacyjne. Na tym etapie prac nad projektem pragniemy przedstawić dwie uwagi o ogólnym charakterze.

1. **Definicja cyberprzestępczości**

Przyjęta definicja cyberprzestępstwa ma kluczowe znaczenie z punktu widzenia praktycznej realizacji Polityki i jej potencjalnego wpływu na poszanowanie praw obywatelskich. Określenie, co jest, a co nie jest cybeprzestępstwem, w oczywisty sposób wpływa na zakres oraz cele działań podejmowanych na etapie wdrożenia Polityki. Naszym zdaniem definicja przyjęta w Polityce ma zbyt ogólny charakter i nie uwzględnia specyfiki środowiska cyfrowego. W związku z tym proponujemy, żeby kolejnym etapem prac nad ostatecznym kształtem Polityki uczynić debatę publiczną na temat **definicji cyberprzestępczości**. W naszej opinii definicja ta nie powinna obejmować działań, które formalnie można zakwalifikować jako naruszenie integralności systemów informatycznych, a które jednocześnie są nieszkodliwe społecznie lub wręcz korzystne dla społeczeństwa.

Z zakresu definicji cyberprzestępstwa wyłączone powinno być np. działanie mające na

celu wytwarzanie narzędzi hakerskich, które nie mają na celu popełnienia przestępstwa, ale mogą służyć np. omijaniu blokad w dostępie do informacji w Internecie lub ukrywaniu tożsamości osób obawiających się represji politycznych. Wymaga to rewizji art. 269b Kodeksu karnego, zgodnie z którym „kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa (…) podlega karze pozbawienia wolności do lat 3". Sposób sformułowania tego przepisu prowadzi do wniosku, że nawet osoba testująca bezpieczeństwo systemów teleinformatycznych za zgodą jego właściciela może być narażony na odpowiedzialność.

Postulujemy również wyraźne wyłączenie karalności działań o charakterze haktywistycznym, tj. manifestacji o charakterze społecznym lub politycznym, polegających np. na modyfikowaniu zawartości stron www, ich podmianie, masowych „odwiedzinach" serwerów w celu ich przeciążenia (DDoS), atakach blokujących lub spowalniających pracę systemów. Działania haktywistyczne od cyberprzestępczości odróżnia bowiem ich wymiar symboliczny: wywołują one skutki jedynie w rzeczywistości wirtualnej, nie prowadzą do poważnych szkód majątkowych ani nie stwarzają zagrożenia dla życia lub zdrowia[1].

W toku prac nad Polityką Ministerstwo powinno zatem uwzględnić istniejące uwarunkowania prawne, a jednocześnie rozważyć możliwość przeprowadzenia niezbędnych zmian legislacyjnych, zgodnych z zasadami przedstawionymi powyżej.

2. Cyberbezpieczeństwo, ale nie za wszelką cenę

Naszym zdaniem troska o cyberbezpieczeństwo nie może realizować się kosztem fundamentalnych wartości, tj. prawa do informacji, wolności słowa czy anonimowości w Internecie. W związku z tym środki, które władze państwowe podejmują w trosce o bezpieczną cyberprzestrzeń, nie mogą opierać się na filtrowaniu i blokowaniu sieci, a także obowiązkowym monitorowaniu zachowań użytkowników.

W tym kontekście przypominamy nasze stanowisko dotyczące „Wytycznych w zakresie ochrony portali informacyjnych administracji publicznej" wydanych przez Ministra Administracji i Cyfryzacji[2]. Zwróciliśmy wówczas uwagę na zakładaną w wytycznych

[1] Problem ten został podniesiony przez Ministra Administracji i Cyfryzacji Michała Boniego podczas Budapeszteńskiej Konferencji o Cyberprzestrzeni, por. http://mac.gov.pl/dzialania/michal-boni-w-budapeszcie-o-ceberbezpieczenstwie/.

[2] Nasze stanowisko dostępne jest na stronie: http://www.panoptykon.org/wiadomosc/nie-zamykajcie-stron-rzadowych-dla-anonimowego-ruchu-ograniczy-nasze-prawa.

możliwość **blokowania dostępu do portali rządowych** osobom, które korzystają z rozwiązań anonimizujących oraz filtrowanie ruchu przychodzącego według bliżej nieokreślonych kryteriów. Naszym zdaniem takie środki (zwłaszcza w kontekście dowolności ich stosowania przez administratorów poszczególnych stron) są nieproporcjonalne do celu i mogą realnie ograniczyć konstytucyjne prawo obywateli do informacji – korzystania z portali informacyjnych administracji publicznej przez osoby, które pragną zachować swoją anonimowość.

Jak słusznie zauważono w projekcie Polityki cyberbezpieczeństwo ma charakter globalny. Aktem prawnym, który w założeniu miał wzmocnić cyberbezpieczeństwo na poziomie międzynarodowym jest Konwencja Rady Europy o cyberprzestępczości. Część postanowień Konwencji ma kontrowersyjny charakter, w związku z czym została ona podpisana i ratyfikowana jedynie przez 33 państwa. Polska podpisała Konwencję, jednak nie została ona do dzisiaj ratyfikowana. Naszym zdaniem w trosce o cyberbezpieczeństwo zarówno na poziome Polski, jak i na poziomie globalnym, a jednocześnie zapewnienie gwarancji praw podstawowych w środowisku cyfrowym, Polska powinna aktywnie zaangażować się w proces rewizji Konwencji, który zapowiadany jest na lata 2012-2015[3]. Natomiast ewentualna ratyfikacja Konwencji powinna być poprzedzona szeroką debatą publiczną oraz konsultacjami społecznymi.

Z wyrazami szacunku,

Katarzyna Szymielewicz
Prezeska Fundacji Panoptykon

[3] Por. https://wcd.coe.int/ViewDoc.jsp?Ref=CM%282011%29175&Language=lanEnglish&Ver=final&BackColorIntern.