P8_TA(2018)0258

Cyberobrona

Rezolucja Parlamentu Europejskiego z dnia 13 czerwca 2018 r. w sprawie cyberobrony (2018/2004(INI))

(2020/C 28/06)

Parlament Europejski,

— uwzględniając Traktat o Unii Europejskiej (TUE) oraz Traktat o funkcjonowaniu Unii Europejskiej (TFUE),

— uwzględniając dokument pt. „Wspólna wizja, wspólne działanie: silniejsza Europa – globalna strategia na rzecz polityki zagranicznej i bezpieczeństwa Unii Europejskiej", przedstawiony przez wiceprzewodniczącą Komisji / wysoką przedstawiciel Unii do spraw zagranicznych i polityki bezpieczeństwa w dniu 28 czerwca 2016 r.,

— uwzględniając konkluzje Rady z dnia 20 grudnia 2013 r., z dnia 26 czerwca 2015 r., z dnia 15 grudnia 2016 r., z dnia 9 marca 2017 r., z dnia 22 czerwca 2017 r., z dnia 20 listopada 2017 r. oraz z dnia 15 grudnia 2017 r.,

— uwzględniając komunikat Komisji z dnia 7 czerwca 2017 r. pt. „Dokument otwierający debatę na temat przyszłości europejskiej obronności" (COM(2017)0315),

— uwzględniając komunikat Komisji z dnia 7 czerwca 2017 r. pt. „Utworzenie Europejskiego Funduszu Obronnego" (COM(2017)0295),

— uwzględniając komunikat Komisji z dnia 30 listopada 2016 r. w sprawie europejskiego planu działań w sektorze obrony (COM(2016)0950),

— uwzględniając wspólny komunikat Komisji / wysokiej przedstawiciel Unii do spraw zagranicznych i polityki bezpieczeństwa z dnia 7 lutego 2013 r. do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń" (JOIN(2013)0001),

— uwzględniając dokument roboczy służb Komisji z dnia 13 września 2017 r. pt. „Ocena strategii cyberbezpieczeństwa Unii Europejskiej 2013" (SWD(2017)0295),

— uwzględniając unijne ramy polityki w zakresie cyberobrony z dnia 18 listopada 2014 r.,

— uwzględniając konkluzje Rady z dnia 10 lutego 2015 r. w sprawie dyplomacji elektronicznej,

— uwzględniając konkluzje Rady z dnia 19 czerwca 2017 r. w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej"),

— uwzględniając wspólny komunikat Komisji / wysokiej przedstawiciel Unii do spraw zagranicznych i polityki bezpieczeństwa z dnia 13 września 2017 r. do Parlamentu Europejskiego i Rady pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej" (JOIN(2017)0450),

— uwzględniając dokument pt. „Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" [Talliński podręcznik 2.0 prawa międzynarodowego mającego zastosowanie w cyberoperacjach] ([1]),

— uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii ([2]),

— uwzględniając prace Światowej Komisji ds. Stabilności w Cyberprzestrzeni,

— uwzględniając komunikat Komisji z dnia 28 kwietnia 2015 r. pt. „Europejska agenda bezpieczeństwa" (COM(2015)0185),

— uwzględniając wspólny komunikat Komisji i wysokiej przedstawiciel Unii Europejskiej do spraw zagranicznych i polityki bezpieczeństwa z dnia 6 kwietnia 2016 r. do Parlamentu Europejskiego i Rady pt. „Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym: odpowiedź Unii Europejskiej" (JOIN(2016)0018),

— uwzględniając swoją rezolucję z dnia 3 października 2017 r. w sprawie walki z cyberprzestępczością ([3]),

— uwzględniając wspólne oświadczenie przewodniczących Rady Europejskiej i Komisji oraz sekretarza generalnego NATO z dnia 8 lipca 2016 r. w sprawie wspólnych zestawów propozycji wdrożenia wspólnego oświadczenia, zatwierdzonych przez Radę UE i Radę Północnoatlantycką NATO w dniach 6 grudnia 2016 r. i 5 grudnia 2017 r. oraz sprawozdań z postępów w ich wdrażaniu z dnia 14 czerwca i z dnia 5 grudnia 2017 r.,

— uwzględniając swoją rezolucję z dnia 22 listopada 2012 r. w sprawie bezpieczeństwa cybernetycznego i cyberobrony ([4]),

— uwzględniając swoją rezolucję z dnia 22 listopada 2016 r. w sprawie Europejskiej Unii Obrony ([5]),

— uwzględniając wniosek Komisji z dnia 13 września 2017 r. dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie „Agencji UE ds. cyberbezpieczeństwa" ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt ws. cyberbezpieczeństwa") (COM(2017)0477),

— uwzględniając swoją rezolucję z dnia 13 grudnia 2017 r. w sprawie sprawozdania rocznego w sprawie realizacji wspólnej polityki zagranicznej i bezpieczeństwa (WPZiB) ([6]),

— uwzględniając swoją rezolucję z dnia 13 grudnia 2017 r. w sprawie sprawozdania rocznego w sprawie wdrażania wspólnej polityki bezpieczeństwa i obrony (WPBiO) ([7]),

— uwzględniając art. 52 Regulaminu,

— uwzględniając sprawozdanie Komisji Spraw Zagranicznych (A8-0189/2018),

A. mając na uwadze, że wyzwania, zagrożenia i ataki cybernetyczne i hybrydowe stanowią poważne zagrożenie dla bezpieczeństwa, obrony, stabilności i konkurencyjności UE, jej państw członkowskich i obywateli; mając na uwadze, że cyberobrona wyraźnie obejmuje zarówno wymiar wojskowy, jak i cywilny;

([1]) Cambridge University Press, luty 2017 r., ISBN 9781316822524, https://doi.org/10.1017/9781316822524.
([2]) Dz.U. L 194 z 19.7.2016, s. 1.
([3]) Teksty przyjęte, P8_TA(2017)0366.
([4]) Dz.U. C 419 z 16.12.2015, s. 145.
([5]) Teksty przyjęte, P8_TA(2016)0435.
([6]) Teksty przyjęte, P8_TA(2017)0493.
([7]) Teksty przyjęte, P8_TA(2017)0492.

B. mając na uwadze, że UE i państwa członkowskie stoją w obliczu bezprecedensowego zagrożenia w formie sponsorowanych przez podmioty państwowe ataków cybernetycznych na tle politycznym, a także cyberprzestępczości i terroryzmu;

C. mając na uwadze, że cyberprzestrzeń jest szeroko uznawana przez służby wojskowe za piątą sferę operacyjną, co umożliwia rozwój zdolności w zakresie cyberobrony; mając na uwadze trwające dyskusje na temat uznania cyberprzestrzeni za piątą sferę prowadzenia wojny;

D. mając na uwadze, że klauzula wzajemnej obrony (art. 42 ust. 7 TUE) stanowi o wzajemnym obowiązku udzielenia pomocy i wsparcia przy zastosowaniu wszelkich dostępnych środków, w przypadku gdy jakiekolwiek państwo członkowskie stanie się ofiarą zbrojnej agresji na jego terytorium; mając na uwadze, że nie ma to wpływu na szczególny charakter polityki bezpieczeństwa i obrony niektórych państw członkowskich; mając na uwadze, że klauzula solidarności zawarta w art. 222 TFUE uzupełnia klauzulę wzajemnej obrony przez wskazanie, że państwa UE mają obowiązek podjęcia wspólnych działań, jeżeli którekolwiek państwo UE stanie się przedmiotem ataku terrorystycznego bądź ofiarą klęski żywiołowej lub katastrofy spowodowanej przez człowieka; mając na uwadze, że klauzula solidarności zakłada wykorzystanie zarówno struktur cywilnych, jak i wojskowych;

E. mając na uwadze, że choć cyberobrona należy do podstawowych kompetencji państw członkowskich, UE ma do odegrania zasadniczą rolę w zapewnieniu platformy dla współpracy na szczeblu europejskim oraz ścisłej koordynacji tych nowych inicjatyw na szczeblu międzynarodowym oraz w ramach architektury bezpieczeństwa transatlantyckiego od samego początku, tak aby zapobiec brakowi skuteczności cechującemu wiele tradycyjnych inicjatyw w zakresie obrony; mając na uwadze, że nasze działania muszą wykraczać poza wzmocnienie współpracy i koordynacji; mając na uwadze, że musimy zapewnić skuteczne zapobieganie poprzez zwiększenie zdolności UE do wykrywania, obrony i powstrzymywania ataków; mając na uwadze, że wiarygodna cyberobrona i cyberprewencja są niezbędne dla osiągnięcia skutecznego cyberbezpieczeństwa dla UE, przy jednoczesnym zagwarantowaniu, by gorzej przygotowane państwa nie stały się łatwym celem dla cyberataków, a także mając na uwadze, że znaczące zdolności w zakresie cyberobrony powinny być niezbędnym elementem WPBiO oraz rozwoju Europejskiej Unii Obrony; mając na uwadze, że znajdujemy się w sytuacji stałego niedoboru wysoko wykwalifikowanych specjalistów w dziedzinie cyberobrony; mając na uwadze, że ścisła koordynacja w zakresie ochrony sił zbrojnych przed atakami cybernetycznymi stanowi niezbędny element rozwoju skutecznej WPBiO;

F. mając na uwadze, że państwa członkowskie UE często są przedmiotem cyberataków przeprowadzanych przez wrogie i niebezpieczne podmioty państwowe i niepaństwowe na cele cywilne lub wojskowe; mając na uwadze, że obecna podatność na zagrożenia wynika głównie z fragmentacji europejskich strategii i zdolności obronnych, umożliwiając zagranicznym agencjom wywiadowczym wielokrotne wykorzystywanie luk w zabezpieczeniach systemów i sieci informatycznych o zasadniczym znaczeniu dla bezpieczeństwa europejskiego; mając na uwadze, że rządy państw członkowskich często nie informowały na czas zainteresowanych stron, aby umożliwić im wyeliminowanie luk w zabezpieczeniach ich produktów i usług; mając na uwadze, że ataki te wymagają pilnego wzmocnienia i rozwoju europejskich zdolności ofensywnych i obronnych na szczeblu cywilnym i wojskowym w celu uniknięcia ewentualnych transgranicznych skutków gospodarczych i społecznych incydentów cybernetycznych;

G. mając na uwadze, że granice między interwencją cywilną a wojskową zacierają się w cyberprzestrzeni;

H. mając na uwadze, że wiele incydentów cybernetycznych wynika z braku odporności i solidności publicznej i prywatnej infrastruktury sieciowej, słabo chronionych lub zabezpieczonych baz danych oraz innych wad krytycznej infrastruktury informacyjnej; mając na uwadze, że jedynie niewiele państw członkowskich bierze odpowiedzialność za ochronę swoich sieci i systemów informacyjnych oraz związanych z nimi danych, w ramach spoczywającego na nich obowiązku należytej staranności, co tłumaczy ogólny brak inwestycji w szkolenia i nowoczesną technologię bezpieczeństwa oraz opracowanie odpowiednich wytycznych;

I. mając na uwadze, że prawa do prywatności i ochrony danych zostały określone w Karcie praw podstawowych UE oraz w art. 16 TFUE i są uregulowane ogólnym rozporządzeniem UE o ochronie danych, które weszło w życie dnia 25 maja 2018 r.;

J. mając na uwadze, że aktywna i skuteczna polityka w zakresie cyberbezpieczeństwa umożliwia odstraszanie wrogów i przełamywanie ich zdolności, uprzedzanie działań oraz ograniczanie ich możliwości dokonania ataku;

K. mając na uwadze, że kilka grup i organizacji terrorystycznych wykorzystuje cyberprzestrzeń jako tanie narzędzie rekrutacji, radykalizacji i szerzenia propagandy terrorystycznej; mając na uwadze, że grupy terrorystyczne, podmioty niepaństwowe i międzynarodowe sieci przestępcze wykorzystują działania cybernetyczne do anonimowego zbierania funduszy, gromadzenia informacji wywiadowczych i opracowywania broni cybernetycznej do prowadzenia kampanii cyberterrorystycznych, zakłócania, uszkodzeń lub niszczenia infrastruktury krytycznej, atakowania systemów finansowych i prowadzenia innych nielegalnych działań wywierających istotny wpływ na bezpieczeństwo europejskich obywateli;

L. mając na uwadze, że cyberprewencja i cyberobrona europejskich sił zbrojnych oraz infrastruktura krytyczna stały się kluczowymi kwestiami w dyskusjach na temat modernizacji sektora obrony, wspólnych europejskich inicjatyw w zakresie obrony, przyszłego rozwoju sił zbrojnych i ich działań oraz strategicznej autonomii Unii Europejskiej;

M. mając na uwadze, że kilka państw członkowskich poczyniło znaczne inwestycje w stworzenie cybernetycznych dowództw dysponujących wykwalifikowanym personelem, aby sprostać tym nowym wyzwaniom i zwiększyć swoją cyberodporność, lecz wciąż wiele pozostaje do zrobienia, ponieważ przeciwdziałanie cyberatakom na szczeblu państw członkowskich jest coraz trudniejsze; mając na uwadze, że dowództwa cybernetyczne poszczególnych państw członkowskich różnią się pod względem mandatu ofensywnego i defensywnego; mając na uwadze, że struktury cyberobrony są dalece zróżnicowane w poszczególnych państwach członkowskich i często pozostają rozdrobione; mając na uwadze, że cyberobrona i cyberprewencja należą do działań, które można najlepiej realizować w ramach współpracy na szczeblu europejskim w koordynacji z naszymi partnerami i sojusznikami, gdyż ich sfera operacyjna nie uznaje żadnych granic – ani krajowych, ani organizacyjnych; mając na uwadze, że cyberbezpieczeństwo wojskowe i cywilne są ze sobą ściśle powiązane, zatem potrzebna jest większa synergia między specjalistami cywilnymi i wojskowymi; mając na uwadze, że prywatne przedsiębiorstwa dysponują dużą wiedzą fachową w tej dziedzinie, co rodzi zasadnicze pytania na temat sprawowania rządów i bezpieczeństwa, a także zdolności państw do obrony swoich obywateli;

N. mając na uwadze, że istnieje nagląca potrzeba wzmacniania zdolności UE w dziedzinie cyberobrony z powodu braku odpowiednio szybkiej reakcji na zmieniający się obraz bezpieczeństwa cybernetycznego; mając na uwadze, że szybkość reakcji i odpowiedni stan gotowości są kluczowymi elementami zapewniającymi bezpieczeństwo w tej sferze;

O. mając na uwadze, że zarówno stała współpraca strukturalna (PESCO), jak i Europejski Fundusz Obronny to nowe inicjatywy obejmujące zakres konieczny dla wspierania ekosystemu zapewniającego możliwości dla MŚP i przedsiębiorstw typu start-up oraz dla wspierania wspólnych projektów w dziedzinie cyberobrony, które to inicjatywy przyczynią się do ukształtowania ram regulacyjnych i instytucjonalnych;

P. mając na uwadze, że państwa członkowskie uczestniczące w PESCO zobowiązały się do dalszego zacieśniania współpracy obejmującej inicjatywy w zakresie cyberobrony, takie jak wymiana informacji, szkolenie i wsparcie operacyjne;

Q. mając na uwadze, że dwa spośród siedemnastu projektów wybranych w ramach PESCO dotyczą cyberobrony;

R. mając na uwadze, że Europejski Fundusz Obronny musi wspierać światową konkurencyjność i innowacyjność europejskiego przemysłu obronnego poprzez inwestycje w technologie cyfrowe i cybernetyczne, a także ułatwiać rozwój inteligentnych rozwiązań poprzez umożliwianie MŚP i przedsiębiorstwom typu start-up uczestnictwa w tych działaniach;

S. mając na uwadze, że Europejska Agencja Obrony (EDA) zainicjowała szereg projektów ukierunkowanych na zaspokojenie potrzeb państw członkowskich w rozwijaniu ich zdolności w zakresie cyberobrony, w tym projektów z zakresu kształcenia i szkolenia, takich jak platforma szkoleń i koordynacji ćwiczeń w dziedzinie cyberobrony (CD TEXP), wsparcie sektora prywatnego dla łączenia zamówień dotyczących szkoleń i ćwiczeń w dziedzinie cyberobrony (DePoCyTE) oraz projekt platform cybernetycznych;

T. mając na uwadze inne bieżące projekty UE w dziedzinie orientacji sytuacyjnej, wykrywania złośliwego oprogramowania i wymiany informacji (platforma wymiany informacji na temat złośliwego oprogramowania (MISP) oraz wielopodmiotowy system wykrywania zaawansowanych, trwałych zagrożeń (MASFAD));

U. mając na uwadze znaczne i rosnące potrzeby szkoleniowe oraz w ramach budowania zdolności w dziedzinie cyberobrony, które najskuteczniej można zaspokoić przez wspólne działania na szczeblu UE i NATO;

V. mając na uwadze, że misje i operacje WPBiO, podobnie jak w przypadku wszystkich nowoczesnych przedsięwzięć organizacyjnych, są głęboko uzależnione od funkcjonowania systemów informatycznych; mając na uwadze, że cyberzagrożenia dla misji i operacji WPBiO mogą wystąpić w różnych warstwach, od warstwy taktycznej (misje i operacje WPBiO) i operacyjnej (sieci UE) po szerszą warstwę ogólnoświatowej infrastruktury informatycznej;

W. mając na uwadze, że systemy dowodzenia i kontroli, wymiana informacji i logistyka opierają się na infrastrukturze informatycznej do przesyłania informacji niejawnych i jawnych, zwłaszcza na poziomie taktycznym i operacyjnym; mając na uwadze, że systemy te są atrakcyjnym celem dla podmiotów działających w złych intencjach, szukających okazji do ataku na misje; mając na uwadze, że cyberataki mogą mieć poważne skutki dla infrastruktury UE; mając na uwadze, że ataki cybernetyczne, zwłaszcza na infrastrukturę energetyczną UE, miałyby poważne konsekwencje, dlatego należy się przed nimi chronić;

X. mając na uwadze, że powszechnie uznaje się, iż cyberobrona powinna być należycie uwzględniana na wszystkich etapach procesu planowania misji i operacji WPBiO i wymaga ciągłego monitorowania oraz że konieczne są odpowiednie zdolności, aby w pełni uwzględniać cyberobronę w planowaniu misji i ustawicznie zapewniać niezbędne kluczowe wsparcie;

Y. mając na uwadze, że sieć Europejskiego Kolegium Bezpieczeństwa i Obrony (EKBiO) jest jedynym europejskim organizatorem szkoleń dla struktur, misji i działań w ramach WPBiO; mając na uwadze, że zgodnie z obecnymi planami jego rola w łączeniu możliwości szkoleniowych w Europie w domenie cyfrowej ma zostać znacznie zwiększona;

Z. mając na uwadze, że w deklaracji ze szczytu NATO w Warszawie w 2016 r. uznano cyberprzestrzeń za sferę operacyjną, w ramach której NATO musi zapewnić równie skuteczną obronę, jak w przypadku działań prowadzonych w powietrzu, na lądzie i na morzu;

AA. mając na uwadze, że UE i NATO przyczyniły się do zwiększenia zdolności państw członkowskich w zakresie cyberobrony, prowadząc projekty badawcze w zakresie produktów podwójnego zastosowania, koordynowane przez EDA i NATO, oraz zwiększając cyberodporność państw członkowskich dzięki wsparciu udzielanemu przez Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA);

AB. mając na uwadze, że w 2014 roku NATO uznało operacje w zakresie cyberbezpieczeństwa za element obrony zbiorowej, a w 2016 roku uznało cyberprzestrzeń za sferę operacyjną wraz z działaniami prowadzonymi na lądzie, w powietrzu i na morzu; mając na uwadze, że UE i NATO są uzupełniającymi się partnerami w procesie budowania swoich zdolności w zakresie cyberodporności i cyberobrony; mając na uwadze, że cyberbezpieczeństwo i cyberobrona już teraz stanowią jeden z najmocniejszych filarów współpracy obu tych podmiotów oraz kluczową dziedzinę, w której obydwa posiadają wyjątkowe zdolności; mając na uwadze, że we wspólnej deklaracji UE–NATO z dnia 8 lipca 2016 r. UE i NATO uzgodniły szeroki program współpracy; mając na uwadze, że cztery spośród 42 wniosków dotyczących zacieśnienia współpracy dotyczą cyberbezpieczeństwa i cyberobrony, a kolejne wnioski ukierunkowane są na szerzej pojęte zagrożenia hybrydowe; mając na uwadze, że towarzyszył im kolejny wniosek dotyczący cyberbezpieczeństwa i cyberobrony, przedstawiony dnia 5 grudnia 2017 r.;

AC. mając na uwadze, że grupa ekspertów rządowych ONZ ds. bezpieczeństwa informacji (UNGGE) zakończyła ostatnią rundę obrad; mając na uwadze, że choć grupa ta nie zdołała opracować sprawozdania kompromisowego w 2017 r., wciąż obowiązują porozumienia z lat 2015 i 2013, uznające m.in., że obowiązujące prawo międzynarodowe – w szczególności Karta Narodów Zjednoczonych – ma zastosowanie i ma zasadnicze znaczenie dla utrzymania pokoju i stabilności oraz wspierania otwartego, bezpiecznego, pokojowego i dostępnego środowiska ICT;

AD. mając na uwadze, że w niedawno wprowadzonych ramach wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne – unijnym zestawie narzędzi dla dyplomacji cyfrowej ukierunkowanym na rozwijanie zdolności UE i państw członkowskich w celu wywierania wpływu na zachowanie potencjalnych agresorów – przewiduje się stosowanie proporcjonalnych środków w ramach WPZiB, w tym środków ograniczających;

AE. mając na uwadze, że różne podmioty państwowe – m.in. Rosja, Chiny i Korea Północna – ale także podmioty niepaństwowe (w tym organizacje przestępcze) inspirowane, wynajmowane lub wspierane przez państwa, agencje bezpieczeństwa lub prywatne przedsiębiorstwa, były zaangażowane w szkodliwe działania cybernetyczne w dążeniu do osiągnięcia celów politycznych, ekonomicznych lub w zakresie bezpieczeństwa, obejmujące ataki na infrastrukturę krytyczną, cyberszpiegostwo i masową inwigilację obywateli UE, umożliwiające prowadzenie kampanii dezinformacyjnych i rozpowszechnianie złośliwego oprogramowania (Wannacry, NotPetya itp.) ograniczającego dostępu do internetu i funkcjonowanie systemów informatycznych; mając na uwadze, że takie działania stanowią lekceważenie i naruszenie prawa międzynarodowego, praw człowieka i praw podstawowych UE, zagrażając demokracji, bezpieczeństwu, porządkowi publicznemu i strategicznej autonomii UE, dlatego powinny powodować wspólną unijną reakcję, np. w ramach wspólnej unijnej reakcji dyplomatycznej, w tym przy użyciu środków ograniczających przewidzianych w unijnym zestawie narzędzi dla dyplomacji cyfrowej, takich jak – w przypadku przedsiębiorstw prywatnych – nakładanie grzywien i ograniczanie dostępu do rynku wewnętrznego;

AF. mając na uwadze, że takie masowe ataki na infrastrukturę informatyczną miały wielokrotnie miejsce w przeszłości, w tym w Estonii w 2007 r., w Gruzji w 2008 r. oraz obecnie niemal każdego dnia na Ukrainie; mając na uwadze, że ofensywne zdolności cybernetyczne są również wykorzystywane przeciw państwom członkowskim UE i NATO na niespotykaną dotąd skalę;

AG. mając na uwadze, że technologie bezpieczeństwa cybernetycznego, mające znaczenie zarówno dla sfery wojskowej, jak i cywilnej, są technologiami podwójnego zastosowania, które oferują wiele możliwości dla wypracowania synergii między podmiotami cywilnymi i wojskowymi w szeregu dziedzin, takich jak szyfrowanie, narzędzia do zarządzania bezpieczeństwem i lukami w zabezpieczeniach, systemy wykrywania włamań i przeciwdziałania im;

AH. mając na uwadze, że rozwój technologii cyfrowych w kolejnych latach będzie wywierać wpływ na nowe dziedziny, w tym sztuczną inteligencję, internet rzeczy, robotykę i urządzenia mobilne, a wszystko to może również mieć poważne konsekwencje dla obszaru obrony;

AI. mając na uwadze, że dowództwa cybernetyczne ustanowione przez wiele państw członkowskich mogą wnieść istotny wkład w ochronę cywilnej infrastruktury krytycznej, oraz mając na uwadze, że wiedza związana z cyberobroną często jest równie przydatna w sferze cywilnej;

Rozwój zdolności w zakresie cyberobrony i cyberprewencji

1. podkreśla, że wspólna polityka i znaczące zdolności w dziedzinie cyberobrony powinny stanowić najważniejsze elementy rozwoju Europejskiej Unii Obrony;

2. przyjmuje z zadowoleniem inicjatywę Komisji dotyczącą pakietu cyberbezpieczeństwa w celu wsparcia cyberodporności, cyberprewencji i cyberobrony UE;

3. przypomina, że cyberobrona ma wymiar zarówno wojskowy, jak i cywilny, co oznacza, że konieczne jest zintegrowane podejście polityczne i ścisła współpraca zainteresowanych podmiotów sektora wojskowego i cywilnego;

4. wzywa do spójnego rozwoju zdolności w zakresie cyberbezpieczeństwa we wszystkich instytucjach i organach UE oraz w państwach członkowskich, a także do zapewnienia niezbędnych rozwiązań politycznych i praktycznych w celu przezwyciężenia pozostałych przeszkód politycznych, ustawodawczych i organizacyjnych dla współpracy w zakresie cyberobrony; uważa, że kluczowe znaczenie ma regularna i pogłębiona wymiana informacji i współpraca między odpowiednimi zainteresowanymi podmiotami sektora publicznego w dziedzinie cyberobrony na szczeblu unijnym oraz krajowym;

5. zdecydowanie podkreśla, że w ramach powstającej Europejskiej Unii Obrony należy od początku wysunąć na pierwszy plan oraz w jak największym zakresie zintegrować zdolności państw członkowskich w zakresie cyberobrony z myślą o zapewnieniu maksymalnej skuteczności; apeluje zatem do państw członkowskich o ścisłą współpracę przy rozwijaniu ich zdolności do cyberobrony przy użyciu jasnego harmonogramu i przez to przyczynienie się do realizacji procesu koordynowanego przez Komisję, Europejską Służbę Działań Zewnętrznych (ESDZ) i EDA w celu usprawnienia struktur cyberobrony w państwach członkowskich, wdrażając dostępne środki krótkoterminowe w trybie pilnym i wspierając wymianę wiedzy specjalistycznej; jest zdania, że powinniśmy opracować bezpieczną sieć europejską w dziedzinie informacji i infrastruktury o znaczeniu krytycznym; uznaje, że silne zdolności w zakresie atrybucji stanowią zasadniczy komponent skutecznej cyberobrony i cyberprewencji oraz że skuteczna profilaktyka będzie wymagała znacznego poszerzenia wiedzy technologicznej; wzywa państwa członkowskie do zwiększenia zasobów finansowych i kadrowych, w szczególności w dziedzinie informatyki śledczej, w celu lepszej atrybucji cyberataków; podkreśla, że taka współpraca powinna być również realizowana przez wzmocnienie ENISA;

6. uznaje fakt, że wiele państw członkowskich uważa, iż posiadanie własnych zdolności w zakresie cyberobrony jest podstawą krajowej strategii bezpieczeństwa i stanowi zasadniczy element suwerenności państw; podkreśla jednak, że ze względu na ponadgraniczny charakter cyberprzestrzeni skala działań i wiedzy wymaganych dla zapewnienia rzeczywiście kompleksowych i skutecznych sił zbrojnych gwarantujących strategiczną autonomię UE w cyberprzestrzeni leży poza zasięgiem możliwości jakiegokolwiek pojedynczego państwa członkowskiego, dlatego sytuacja ta wymaga zdecydowanej i skoordynowanej reakcji ze strony wszystkich państw członkowskich na szczeblu UE; w tym kontekście zauważa, że UE i państwa członkowskie znajdują się pod presją czasu w odniesieniu do wypracowania takich sił, co wymaga podjęcia niezwłocznych działań; zauważa, że dzięki takim unijnym inicjatywom jak jednolity rynek cyfrowy UE jest dobrze przygotowana do objęcia wiodącej roli w opracowywaniu europejskich strategii w dziedzinie cyberobrony; przypomina, że rozwój cyberobrony na szczeblu UE musi zwiększać jej zdolność do własnej ochrony; w tym kontekście przyjmuje z zadowoleniem wniosek w sprawie stałego mandatu i wzmocnionej roli agencji ENISA;

7. w tym kontekście wzywa państwa członkowskie, by przy zgłaszaniu projektów współpracy jak najlepiej wykorzystywały ramy udostępnione przez PESCO i EFR;

8. odnotowuje ciężką pracę wykonaną przez EU i państwa członkowskie w dziedzinie cyberobrony; zwraca w szczególności uwagę na projekty EDA obejmujące platformy cybernetyczne, program badań strategicznych w zakresie cyberobrony oraz opracowanie nadających się do zastosowania pakietów orientacji sytuacyjnej w cyberprzestrzeni, przeznaczonych dla sztabów;

9. z zadowoleniem przyjmuje dwa projekty cybernetyczne, które mają zostać zainicjowane w ramach PESCO, a mianowicie platformę wymiany informacji na temat cyberzagrożeń i reagowania na incydenty cybernetyczne, zespoły szybkiego reagowania cybernetycznego oraz projekt wzajemnej pomocy w dziedzinie cyberbezpieczeństwa; podkreśla, że te dwa projekty skupione są na defensywnej polityce cybernetycznej, która opiera się na wymianie informacji na temat cyberzagrożeń za pomocą połączonej w sieć platformy państw członkowskich oraz na powołaniu zespołów szybkiego reagowania cybernetycznego, umożliwiając państwom członkowskim niesienie wzajemnej pomocy w celu zapewnienia wyższego poziomu cyberodporności oraz wspólnego wykrywania, rozpoznawania i łagodzenia cyberzagrożeń; wzywa Komisję i państwa członkowskie do wykorzystania projektów PESCO dotyczących krajowych zespołów szybkiego reagowania cybernetycznego i wzajemnej pomocy w dziedzinie cyberbezpieczeństwa przez ustanowienie europejskiego zespołu szybkiego reagowania cybernetycznego, którego zadaniem byłoby koordynowanie i wykrywanie zbiorowych cyberzagrożeń oraz przeciwdziałanie im w celu wsparcia działań uczestniczących państw członkowskich;

10. zwraca uwagę, że zdolność UE do opracowywania projektów w dziedzinie cyberobrony zależy od opanowania technologii, sprzętu, usług, danych i ich przetwarzania oraz powinna opierać się na zaufanych przedsiębiorstwach przemysłowych;

11. przypomina, że wysiłki podejmowane na rzecz poprawy spójności systemów dowodzenia mają na celu między innymi osiągnięcie interoperacyjności dostępnych zasobów dowodzenia z zasobami zarówno państw członkowskich NATO nienależących do UE, jak i doraźnych partnerów, zapewnienie płynnej wymiany informacji w celu przyspieszenia procesu decyzyjnego oraz zachowanie kontroli nad informacjami w kontekście ryzyka w cyberprzestrzeni;

12. zaleca poszukiwanie sposobów na uzupełnienie projektów NATO w zakresie inteligentnej obrony (np. rozwój wielonarodowych zdolności do cyberobrony, platforma wymiany informacji na temat złośliwego oprogramowania (MISP) oraz międzynarodowe szkolenia i ćwiczenia w zakresie cyberobrony (MNCDE&T));

13. dostrzega postępy zachodzące w dziedzinach takich jak nanotechnologia, sztuczna inteligencja, duże zbiory danych, zużyty sprzęt elektryczny i elektroniczny oraz zaawansowana robotyka; wzywa państwa członkowskie i UE do zwrócenia szczególnej uwagi na możliwości wykorzystywania tych dziedzin przez wrogie podmioty państwowe i zorganizowane grupy przestępcze; apeluje o opracowanie szkoleń i rozwój zdolności w celu zapewnienia ochrony przed powstawaniem wyszukanych schematów przestępczych, takich jak złożone oszustwa dotyczące tożsamości i podrabianie produktów;

14. podkreśla potrzebę większej jasności terminologicznej w dziedzinie bezpieczeństwa w cyberprzestrzeni oraz kompleksowego i zintegrowanego podejścia i wspólnych wysiłków na rzecz przeciwdziałania zagrożeniom cybernetycznym i hybrydowym w celu wykrywania i eliminowania bezpiecznych schronień dla ekstremistów i przestępców w internecie, przez wzmocnienie i zwiększenie wymiany informacji między UE a agencjami UE, takimi jak Europol, Eurojust, EDA i ENISA;

15. podkreśla coraz większą rolę sztucznej inteligencji zarówno w ofensywie, jak i defensywie cybernetycznej; wzywa UE i państwa członkowskie do zwrócenia szczególnej uwagi na ten obszar zarówno w trakcie prac badawczych, jak i na etapie praktycznego rozwoju swych zdolności cyberobrony;

16. zdecydowanie podkreśla, że wykorzystywanie uzbrojonych lub nieuzbrojonych bezzałogowych statków powietrznych wymaga podjęcia dodatkowych środków w celu ograniczenia związanych z nimi potencjalnych cyberzagrożeń;

Cyberobrona misji i operacji WPBiO

17. podkreśla, że w ramach misji i operacji WPBiO należy uznać cyberobronę za zadanie operacyjne, które uwzględnia się we wszystkich procesach planowania dotyczących WPBiO, aby zapewnić nieprzerwane uwzględnianie cyberbezpieczeństwa na wszystkich etapach procesu planowania oraz ograniczać w ten sposób luki w obszarze cyberbezpieczeństwa;

18. przyznaje, że planowanie uwieńczonych powodzeniem misji lub operacji WPBiO wymaga znacznego zasobu wiedzy specjalistycznej w dziedzinie cyberobrony oraz bezpiecznej infrastruktury i sieci informatycznych, zarówno w dowództwie operacji, jak i w samej misji, przeprowadzenia szczegółowej oceny zagrożenia i zapewnienia odpowiedniej ochrony w terenie; apeluje do ESDZ i państw członkowskich zapewniających siedzibę dowództwa operacji WPBiO o zwiększenie wiedzy specjalistycznej w dziedzinie cyberobrony na rzecz misji i operacji UE; zauważa ograniczone możliwości dobrego przygotowania misji WPBiO w celu ochrony przed cyberatakami;

19. podkreśla, że wszelkiemu planowaniu misji i operacji WPBiO musi towarzyszyć szczegółowa ocena krajobrazu cyberzagrożeń; zauważa, że taksonomia zagrożeń opracowana przez ENISA zapewnia odpowiedni szablon dla takiej oceny; zaleca stworzenie zdolności do oceny cyberodporności dla dowództwa WPBiO;

20. uznaje w szczególności znaczenie ograniczenia do niezbędnego minimum śladów cyfrowych i obszaru ataku na misje i operacje WPBiO; wzywa planistów uczestniczących w procesie planowania do uwzględnienia tego wymogu od początku procesu;

21. uznaje analizę potrzeb szkoleniowych EDA, w której wskazano istotne braki w umiejętnościach i kompetencjach w dziedzinie cyberobrony wśród decydentów – nie tylko w państwach członkowskich – i przyjmuje z zadowoleniem inicjatywy EDA dotyczące kursów dla wysokiej rangi decydentów jako wsparcia planowania misji i operacji WPBiO;

Edukacja i szkolenie w dziedzinie cyberobrony

22. zauważa, że usprawniony zestaw unijnych działań edukacyjnych i szkoleniowych w dziedzinie cyberobrony umożliwiłby znaczne złagodzenie zagrożeń i wzywa UE oraz państwa członkowskie do zacieśnienia współpracy w ramach kształcenia, szkoleń i ćwiczeń;

23. zdecydowanie popiera program „wojskowy Erasmus" i inne wspólne inicjatywy w dziedzinie szkoleń i wymiany, których celem jest zwiększenie interoperacyjności sił zbrojnych państw członkowskich i rozwój wspólnej kultury strategicznej przez zwiększenie wymiany młodego personelu wojskowego, biorąc pod uwagę fakt, że tego rodzaju interoperacyjność jest niezbędna wśród wszystkich państw członkowskich i sojuszników NATO; uważa jednak, że wymiany szkoleniowe i edukacyjne w dziedzinie cyberobrony powinny wykraczać poza tę inicjatywę i obejmować personel wojskowy w każdym przedziale wiekowym i wszystkich stopni, a także studentów wszystkich akademickich ośrodków badań nad cyberbezpieczeństwem;

24. podkreśla konieczność zwiększenia liczby specjalistów w dziedzinie cyberobrony; wzywa państwa członkowskie do ułatwienia współpracy między instytucjami akademickimi i akademiami wojskowymi, aby stwarzać większe możliwości w zakresie edukacji i szkolenia w dziedzinie cyberobrony oraz przeznaczać większe zasoby na specjalistyczne szkolenia w dziedzinie operacji cybernetycznych, w tym w zakresie sztucznej inteligencji; wzywa akademie wojskowe do włączenia edukacji w dziedzinie cyberobrony do swych programów kształcenia, tym samym zwiększając pulę talentów w dziedzinie technologii cyfrowych na potrzeby misji WPBiO;

25. wzywa wszystkie państwa członkowskie do dostatecznego i proaktywnego udzielania informacji i zapewniania porad na rzecz przedsiębiorstw, szkół i obywateli oraz podnoszenia ich świadomości na temat cyberbezpieczeństwa i najważniejszych zagrożeń cyfrowych; w tym kontekście z zadowoleniem przyjmuje wytyczne dotyczące cyberbezpieczeństwa jako narzędzia, których celem jest ukierunkowanie obywateli i organizacji na lepsze strategie w dziedzinie cyberbezpieczeństwa, zapewnienie większej wiedzy w tym zakresie i zwiększenie powszechnej cyberodporności;

26. zauważa, że z uwagi na potrzebę bardziej wykwalifikowanych pracowników uwaga państw członkowskich powinna być skupiona nie tylko na rekrutacji kompetentnych pracowników sił zbrojnych, ale także na zatrzymywaniu potrzebnych specjalistów;

27. z zadowoleniem przyjmuje wdrożenie przez 11 państw członkowskich (Austrię, Belgię, Niemcy, Estonię, Grecję, Finlandię, Irlandię, Łotwę, Holandię, Portugalię i Szwecję), które uczestniczą w projekcie Federacji Platform Cybernetycznych, pierwszego z czterech projektów w zakresie cyberobrony, zainicjowanych w ramach programu EDA wspólnego pozyskiwania i wykorzystywania zdolności wojskowych; wzywa pozostałe państwa członkowskie do przyłączenia się do tej inicjatywy; apeluje do państw członkowskich o wspieranie większej wzajemnej dostępności wirtualnych szkoleń w zakresie cyberobrony oraz platform cybernetycznych; zauważa, że w tym kontekście należy również uwzględnić rolę i wiedzę fachową agencji ENISA;

28. uważa, że takie inicjatywy przyczyniają się do podniesienia jakości edukacji w dziedzinie cyberobrony na szczeblu UE, w szczególności przez tworzenie kompleksowych platform technicznych i ustanowienie społeczności ekspertów unijnych; uważa, że europejskie siły zbrojne mogą zwiększyć swą atrakcyjność przez oferowanie kompleksowych szkoleń w dziedzinie cyberobrony, aby przyciągnąć i zatrzymać talenty cyberbernetyczne; podkreśla potrzebę wskazywania słabości systemów komputerowych zarówno państw członkowskich, jak i instytucji UE; przyznaje, że błąd ludzki jest jedną z najczęściej identyfikowanych słabości systemów cyberbezpieczeństwa, dlatego wzywa do regularnych szkoleń zarówno personelu wojskowego, jak i cywilnego pracującego dla instytucji UE;

29. apeluje do EDA o jak najszybsze wprowadzenie platformy szkoleń i koordynacji ćwiczeń w dziedzinie cyberobrony (CD TEXP) w celu wspierania federacji platform cybernetycznych, skupiając uwagę na zacieśnieniu współpracy w zakresie zharmonizowanych wymagań, wspieraniu badań i innowacji technologicznych w dziedzinie cyberobrony oraz niesieniu wspólnej pomocy państwom trzecim w procesie budowania ich zdolności na rzecz osiągnięcia odporności w dziedzinie cyberobrony; apeluje do Komisji i państw członkowskich, aby uzupełniły te inicjatywy o specjalne europejskie centrum doskonałości na rzecz szkoleń w dziedzinie cyberobrony w celu zapewnienia specjalistycznego szkolenia dla najbardziej obiecujących rekrutów, wspierając szkolenia w dziedzinie cyberbezpieczeństwa prowadzonego przez uczestniczące państwa członkowskie;

30. z zadowoleniem przyjmuje ustanowienie w ramach EKBiO platformy edukacji, szkoleń i ćwiczeń oraz oceny w dziedzinie cyberobrony (ETEE) w celu rozwoju możliwości szkoleniowych i edukacyjnych w państwach członkowskich;

31. zachęca do częstszej wymiany informacji w dziedzinie orientacji sytuacyjnej w drodze symulacyjnych ćwiczeń w obszarze cyberbezpieczeństwa i koordynacji wysiłków na rzecz rozwoju odpowiednich zdolności w celu osiągnięcia większej interoperacyjności i lepszego przeciwdziałania przyszłym atakom i reagowania na nie; wzywa do prowadzenia takich projektów we współpracy z sojusznikami NATO, siłami zbrojnymi państw członkowskich UE i innymi partnerami mającymi szerokie doświadczenie w przeciwdziałaniu cyberatakom w celu rozwoju gotowości operacyjnej, wypracowania wspólnych procedur i standardów, aby umożliwić kompleksowe stawianie czoła różnym cyberzagrożeniom; w tym kontekście z zadowoleniem przyjmuje zaangażowanie UE w ćwiczenia w dziedzinie cyberbezpieczeństwa, takie jak ćwiczenie w dziedzinie cyberofensywy i cyberobrony (CODE);

32. przypomina, że odporna cyberprzestrzeń wymaga nienagannej higieny cyberbezpieczeństwa; wzywa wszystkie publiczne i prywatne zainteresowane strony do przeprowadzania regularnych szkoleń w dziedzinie higieny cyberbezpieczeństwa dla wszystkich pracowników;

33. zaleca zwiększenie wymiany wiedzy fachowej oraz wdrożonych doświadczeń i wniosków między siłami zbrojnymi, służbami policyjnymi i innymi organami państwowymi działającymi w państwach członkowskich i zaangażowanymi aktywnie w zwalczanie cyberzagrożeń;

Współpraca UE-NATO w dziedzinie cyberobrony

34. powtarza, że ze względu na wspólne wartości i strategiczne interesy na UE i NATO spoczywa szczególna odpowiedzialność i dysponują one zdolnościami, aby skuteczniej i w ścisłej współpracy reagować na rosnące wyzwania dotyczące cyberbezpieczeństwa i cyberobrony przez poszukiwanie możliwej komplementarności, unikanie powielania działań i uwzględnienie swoich odpowiednich obowiązków;

35. apeluje do Rady, aby we współpracy z innymi właściwymi instytucjami i strukturami UE rozważyła sposoby jak najszybszego zapewnienia wsparcia na szczeblu Unii na rzecz integracji domeny cyfrowej w doktrynach wojskowych państw członkowskich, w zharmonizowany sposób oraz przy ścisłej współpracy z NATO;

36. wzywa do wdrożenia tych środków, które zostały już uzgodnione; apeluje o wskazanie nowych inicjatyw na rzecz dalszej współpracy między UE i NATO, również z uwzględnieniem możliwości współpracy w ramach Centrum Doskonałości NATO ds. Współpracy w Dziedzinie Obrony przed Atakami Cybernetycznymi (CCD COE) oraz Akademii NATO ds. Komunikacji i Informacji (NCI), których celem jest zwiększenie zdolności szkoleniowych w dziedzinie cyberobrony w odniesieniu do informatyki i systemów cybernetycznych, zarówno pod względem sprzętu, jak i oprogramowania komputerowego; zauważa, że mogłoby to obejmować dialog z NATO na temat możliwości dołączenia UE do Centrum w celu zwiększenia komplementarności i zacieśnienia współpracy; z zadowoleniem przyjmuje niedawne utworzenie Europejskiego Centrum ds. Zwalczania Zagrożeń Hybrydowych; wzywa wszystkie odpowiednie instytucje i sojuszników do odbywania regularnych spotkań w celu omawiania wykonywanych działań, aby uniknąć ich pokrywania się i zachęcić do przyjęcia skoordynowanego podejścia do cyberobrony; uważa, że należy stymulować, w oparciu o wzajemne zaufanie, wymianę informacji na temat cyberzagrożeń między państwami członkowskimi a NATO;

37. jest przekonany, że zacieśnienie współpracy między UE i NATO jest ważne i przydatne w dziedzinie cyberobrony w celu wykrywania i powstrzymywania cyberataków oraz zapobiegania im; w związku z tym apeluje do obydwu organizacji o zacieśnienie współpracy i koordynacji operacyjnej oraz o rozszerzenie wspólnych działań w zakresie budowania zdolności, zwłaszcza w postaci wspólnych ćwiczeń i szkoleń personelu cywilnego i wojskowego zaangażowanego w cyberobronę oraz poprzez uczestnictwo państw członkowskich w projektach NATO w dziedzinie inteligentnej obrony; uważa, że niezwykle istotne jest zwiększenie wymiany informacji między UE i NATO w celu umożliwienia formalnej atrybucji cyberataków i w efekcie nakładania restrykcyjnych sankcji na podmioty odpowiedzialne za cyberataki; wzywa obie organizacje do ściślejszej współpracy również w odniesieniu do aspektów zarządzania kryzysowego związanych z cyberbezpieczeństwem;

38. z zadowoleniem przyjmuje wymianę koncepcji na rzecz włączenia wymagań i standardów w dziedzinie cyberobrony do planowania i przeprowadzania misji i operacji w celu zwiększenia interoperacyjności i wyraża nadzieję, że umożliwi to zwiększenie operacyjnego charakteru współpracy na rzecz zapewnienia aspektów dotyczących cyberobrony w ramach odpowiednich misji oraz synchronizację podejścia operacyjnego;

39. z zadowoleniem przyjmuje porozumienie zawarte między unijnym zespołem reagowania na incydenty komputerowe (CERT-EU) i jednostką NATO odpowiadającą za zdolności reagowania na incydenty komputerowe (NCIRC), którego celem jest wspieranie wymiany informacji, udzielanie wsparcia logistycznego, wspólne oceny zagrożeń, pozyskiwanie personelu i wymiana najlepszych praktyk, a wszystko to w celu zapewnienia zdolności do reagowania na zagrożenia w czasie rzeczywistym; podkreśla znaczenie zachęcania do wymiany informacji między CERT-UE i NCIRC oraz działania na rzecz podniesienia poziomu zaufania; jest zdania, że zakłada się, iż informacje posiadane przez CERT-EU mogłyby być przydatne dla badań w dziedzinie cyberobrony oraz dla NATO, a zatem informacje te powinny być udostępniane, pod warunkiem zapewnienia pełnej zgodności z prawodawstwem UE w dziedzinie ochrony danych;

40. z zadowoleniem przyjmuje współpracę między obydwoma organizacjami obejmującą ćwiczenia w zakresie cyberobrony; zwraca uwagę na udział przedstawicieli UE w corocznych ćwiczeniach „Cyber Coalition"; docenia postępy dotyczące udziału UE w ćwiczeniach zarządzania kryzysowego NATO w 2017 r. w ramach równoległych i skoordynowanych ćwiczeń (PACE) w 2017 r. i z zadowoleniem przyjmuje zwłaszcza uwzględnienie elementu cyberobrony; wzywa obie organizacje do wzmożenia starań w tym zakresie;

41. apeluje do UE i NATO o organizowanie regularnych ćwiczeń szczebla strategicznego z udziałem czołowych przywódców politycznych obydwu organizacji; z zadowoleniem przyjmuje w związku z tym estońskie ćwiczenia EU CYBRID 2017, kiedy to po raz pierwszy sekretarz generalny NATO uczestniczył w ćwiczeniach UE;

42. zwraca uwagę, że istnieją znaczne możliwości opracowania bardziej ambitnego i szczegółowego programu współpracy w zakresie cyberobrony, wykraczającego poza współpracę na poziomie koncepcyjnym w kontekście określonych operacji; wzywa obie organizacje do konkretnego i skutecznego wdrożenia istniejących już rozwiązań oraz do przedstawienia bardziej ambitnych wniosków dotyczących kolejnego przeglądu wdrożenia wniosków ze wspólnego oświadczenia;

43. z zadowoleniem przyjmuje ustanowione w 2014 r. Partnerstwo Cybernetyczne NATO z Sektorem Przemysłu (NICP) i apeluje o zaangażowanie UE we współpracę w ramach NICP w celu stworzenia powiązań między współpracą NATO-UE a wiodącymi podmiotami przemysłowymi wyspecjalizowanymi w technologiach cyfrowych z myślą o poprawie cyberbezpieczeństwa w drodze ciągłej współpracy, ze zwróceniem szczególnej uwagi na: szkolenia, ćwiczenia i edukację zarówno dla NATO i UE, jak i przedstawicieli przemysłu; uwzględnienie UE i przemysłu w projektach NATO dotyczących inteligentnej obrony; opartą na współpracy wymianę informacji i najlepszych praktyk dotyczących gotowości i przywracania sprawności między NATO, UE i przemysłem; dążenie do wspólnie rozwijanych zdolności w zakresie cyberobrony; oparte na współpracy reagowanie na cyberincydenty w razie potrzeby i tam, gdzie będzie to możliwe;

44. odnotowuje bieżące prace nad wnioskiem dotyczącym rozporządzenia zmieniającego rozporządzenie w sprawie ENISA ((UE) nr 526/2013) i ustanawiającego europejskie ramy certyfikacji i oznakowania bezpieczeństwa ICT; wzywa agencję ENISA do podpisania porozumienia z NATO na rzecz zwiększenia praktycznej współpracy tych dwóch podmiotów, w tym wymiany informacji i udziału w ćwiczeniach w dziedzinie cyberobrony;

Normy międzynarodowe mające zastosowanie do cyberprzestrzeni

45. wzywa do włączenia zdolności w zakresie cyberobrony do WPZiB oraz do działań zewnętrznych UE i jej państw członkowskich jako zadania przekrojowego, apeluje także o lepsze koordynowanie cyberobrony przez państwa członkowskie, instytucje UE, NATO, ONZ, Stany Zjednoczone i innych partnerów strategicznych, szczególnie w odniesieniu do zasad, norm i środków egzekucyjnych w cyberprzestrzeni;

46. wyraża ubolewanie, że po kilku miesiącach negocjacji grupie ekspertów rządowych ONZ (UNGGE) prowadzącej prace w latach 2016–2017 nie udało się sporządzić nowego sprawozdania kompromisowego; przypomina, że zgodnie ze sprawozdaniem z 2013 r. obowiązujące prawo międzynarodowe, a w szczególności Karta Narodów Zjednoczonych – zakazujące stosowania groźby lub użycia siły przeciwko niezawisłości politycznej któregokolwiek państwa, w tym cybernetycznych operacji wywierania przymusu, mających na celu zakłócenie funkcjonowania infrastruktury technicznej niezbędnej do przeprowadzania oficjalnych procedur partycypacyjnych, w tym wyborów, w innym państwie – ma zastosowanie i powinno być egzekwowane w cyberprzestrzeni; zauważa, że sprawozdanie UNGGE z 2015 r. zawiera zestaw norm dotyczących odpowiedzialnego zachowania państwa, w tym zakazu prowadzenia lub świadomego wspierania przez państwa działań cybernetycznych sprzecznych z ciążącymi na państwach zobowiązaniami wynikającymi z przepisów międzynarodowych; wzywa UE do objęcia wiodącej roli w bieżących i przyszłych dyskusjach na temat międzynarodowych norm obowiązujących w cyberprzestrzeni oraz ich wdrażania;

47. zwraca uwagę na znaczenie tallińskiego podręcznika 2.0 jako podstawy do dyskusji i analizę możliwości stosowania prawa międzynarodowego w odniesieniu do cyberprzestrzeni; wzywa państwa członkowskie do przystąpienia do analizy i stosowania zaleceń określonych przez ekspertów w tallińskim podręczniku, a także do uzgodnienia dalszych dobrowolnych norm międzynarodowego postępowania; w szczególności zauważa, że wszelkie ofensywne wykorzystanie zdolności cybernetycznych powinno opierać się na prawie międzynarodowym;

48. potwierdza pełne zaangażowanie w otwartą, wolną, stabilną i bezpieczną cyberprzestrzeń, cechującą się poszanowaniem podstawowych wartości demokracji, praw człowieka i praworządności, w której spory międzynarodowe rozwiązuje się na drodze pokojowej w oparciu o Kartę Narodów Zjednoczonych i zasady prawa międzynarodowego; apeluje do państw członkowskich o wspieranie dalszego wdrażania wspólnego i kompleksowego unijnego podejścia do dyplomacji cyfrowej i obowiązujących norm w dziedzinie cyberbezpieczeństwa oraz opracowania we współpracy z NATO kryteriów i definicji cyberataku obowiązujących na szczeblu UE w celu zwiększenia zdolności UE do szybkiego osiągania wspólnego stanowiska w odpowiedzi na działanie niezgodne z prawem międzynarodowym w postaci cyberataku; zdecydowanie popiera wdrożenie wskazanych w sprawozdaniu UNGGE z 2015 r. dobrowolnych, niewiążących norm odpowiedzialnego zachowania się państw w cyberprzestrzeni obejmujących poszanowanie prywatności obywateli oraz ich praw podstawowych, jak również utworzenie regionalnych środków budowy zaufania; w tym kontekście popiera prace Światowej Komisji ds. Stabilności w Cyberprzestrzeni na rzecz opracowania wniosków dotyczących norm i polityki na rzecz zwiększenia międzynarodowego bezpieczeństwa i stabilności oraz ukierunkowania odpowiedzialnego zachowania podmiotów państwowych i niepaństwowych w cyberprzestrzeni; popiera wniosek, zgodnie z którym podmioty państwowe i niepaństwowe nie powinny prowadzić działalności celowo i znacząco naruszającej ogólną dostępność lub integralny charakter publicznych kluczowych zasobów internetu, a przez to naruszającej stabilność cyberprzestrzeni, ani świadomie zezwalać na taką działalność;

49. uznaje fakt, że większość infrastruktury technologicznej jest w posiadaniu sektora prywatnego lub jest obsługiwana przez ten sektor, dlatego ścisła współpraca, konsultacje i uwzględnienie sektora prywatnego i grup społeczeństwa obywatelskiego w drodze wielostronnego dialogu ma zasadnicze znaczenie dla zapewnienia otwartej, wolnej, stabilnej i bezpiecznej cyberprzestrzeni;

50. przyznaje, że ze względu na trudności w egzekwowaniu prawa dwustronne umowy między państwami nie zawsze przynoszą oczekiwane efekty; w związku z tym uważa, że budowanie koalicji w ramach grup państw, które zajmują podobne stanowisko i zmierzają do osiągnięcia konsensusu, stanowi skuteczną formę uzupełnienia działań wielu zainteresowanych stron; podkreśla ważną rolę organów lokalnych w procesie innowacji technologicznej i wymiany danych, jeśli chodzi o nasilenie walki z przestępczością i działalnością terrorystyczną;

51. przyjmuje z zadowoleniem przyjęcie przez Radę ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne – tzw. unijnego zestawu narzędzi dla dyplomacji cyfrowej; popiera możliwość podjęcia przez UE restrykcyjnych środków wobec przeciwników dokonujących ataków na jej państwa członkowskie w cyberprzestrzeni, w tym możliwość nakładania sankcji;

52. wzywa również do przyjęcia wyraźnie proaktywnego podejścia do cyberbezpieczeństwa i cyberobrony oraz do powszechnego wzmocnienia dyplomacji cybernetycznej jako przekrojowego zadania w ramach polityki zagranicznej UE oraz jej zdolności i instrumentów, tak aby mogły skutecznie wspierać normy i wartości UE, a także utorować drogę do konsensusu na temat zasad, norm i środków egzekucyjnych w cyberprzestrzeni; zauważa, że budowanie cyberodporności państw trzecich przyczynia się do osiągnięcia międzynarodowego pokoju i bezpieczeństwa, co ostatecznie zapewnia większe bezpieczeństwo europejskich obywateli;

53. uważa, że cyberataki, takie jak NotPetya i WannaCry, są kierowane przez państwo lub odbywają się za wiedzą i zgodą państwa; zauważa, że te cyberataki, które powodują poważne i trwałe szkody gospodarcze, a także są zagrożeniem dla życia, stanowią wyraźne naruszenie międzynarodowego prawa i norm prawnych; uważa zatem, że ataki NotPetya i WannaCry stanowią przypadki naruszenia prawa międzynarodowego, za które odpowiedzialne są odpowiednio Federacja Rosyjska i Korea Północna, i że te dwa państwa powinny spotkać się z proporcjonalną i stosowną reakcją UE i NATO;

54. apeluje o to, by centrum ds. walki z cyberprzestępczością Europolu stało się punktem kontaktowym dla jednostek egzekwowania prawa i agencji rządowych poświęconym kwestiom cyberprzestępczości, którego głównym obowiązkiem byłoby zarządzanie obroną zarówno domen .eu, jak i infrastruktury krytycznej unijnych sieci w czasie ataku; podkreśla, że taki punkt kontaktowy powinien być również uprawniony do wymiany informacji i niesienia pomocy państwom członkowskim;

55. podkreśla znaczenie opracowania norm dotyczących prywatności i bezpieczeństwa, szyfrowania, mowy nienawiści, dezinformacji i zagrożeń terrorystycznych;

56. zaleca, aby każde państwo członkowskie przyjęło obowiązek pomocy każdemu innemu państwu członkowskiemu będącemu ofiarą cyberataku oraz zapewnienia krajowej odpowiedzialności za kwestie cyberbezpieczeństwa w ścisłej współpracy z NATO;

Współpraca cywilno-wojskowa

57. apeluje do wszystkich zainteresowanych podmiotów o wspieranie partnerstw na rzecz transferu wiedzy, wdrażanie odpowiednich modeli biznesowych i zwiększanie zaufania między przedsiębiorstwami oraz użytkownikami końcowymi z sektora obrony i cywilami, a także o lepsze przekładanie wiedzy akademickiej na rozwiązania praktyczne w dążeniu do zapewnienia synergii i przenoszenia rozwiązań między rynkami cywilnymi i wojskowymi – w istocie do jednolitego rynku cyberbezpieczeństwa i produktów z dziedziny cyberbezpieczeństwa, w oparciu o przejrzyste procedury i przy poszanowaniu prawa unijnego i międzynarodowego, z myślą o zachowaniu i wzmocnieniu strategicznej autonomii UE; zauważa kluczową rolę prywatnych przedsiębiorstw z branży cyberbezpieczeństwa w procesie wczesnego ostrzegania przed cyberatakami i ich atrybucji;

58. stanowczo podkreśla znaczenie badań i rozwoju, zwłaszcza w świetle wysokiego poziomu wymagań bezpieczeństwa na rynku obrony; wzywa UE i państwa członkowskie do zapewnienia większego praktycznego wsparcia europejskiej branży cyberbezpieczeństwa i odpowiednim podmiotom gospodarczym, ograniczenia obciążeń biurokratycznych, w szczególności dla MŚP i przedsiębiorstw typu start-up (głównych źródeł innowacyjnych rozwiązań w dziedzinie cyberobrony), a także do propagowania ściślejszej współpracy z uniwersyteckimi organizacjami badawczymi i dużymi podmiotami, w dążeniu do zmniejszenia zależności od produktów cyberbezpieczeństwa ze źródeł zewnętrznych i utworzenia strategicznego łańcucha dostaw na terytorium UE w celu wzmocnienia swej strategicznej autonomii; w związku z tym zwraca uwagę na cenny wkład, który może wnieść EFR i inne instrumenty ujęte w wieloletnich ramach finansowych (WRF);

59. zachęca Komisję do włączenia elementów cyberobrony do sieci europejskich centrów kompetencji i badań w dziedzinie cyberbezpieczeństwa, również z myślą o zapewnieniu dostatecznych zasobów dla zdolności i technologii cybernetycznych podwójnego zastosowania w następnych WRF;

60. zwraca uwagę, że ochrona krytycznych aktywów związanych z infrastrukturą publiczną i inną infrastrukturą cywilną, zwłaszcza systemów informatycznych i związanych z nimi danych, staje się dla państw członkowskich kluczowym zadaniem w dziedzinie obrony, a w szczególności dla organów odpowiedzialnych za bezpieczeństwo systemów informatycznych, oraz że powinna ona wejść w zakres kompetencji albo krajowych struktur cyberobrony, albo wspomnianych organów; podkreśla, że będzie to wymagało odpowiedniego poziomu zaufania i możliwie najściślejszej współpracy między podmiotami wojskowymi, agencjami cyberobrony, innymi właściwymi organami oraz branżami, których to dotyczy, co można osiągnąć tylko poprzez precyzyjne określenie obowiązków, ról i odpowiedzialności podmiotów cywilnych i wojskowych, oraz wzywa wszystkie zainteresowane strony do uwzględnienia tych czynników w swoich procesach planowania; wzywa do zacieśnienia współpracy transgranicznej, przy pełnym poszanowaniu prawodawstwa UE w dziedzinie ochrony danych, w odniesieniu do egzekwowania prawa dotyczącego zwalczania szkodliwych działań cybernetycznych;

61. wzywa wszystkie państwa członkowskie do ukierunkowania krajowych strategii cyberbezpieczeństwa na ochronę systemów informacyjnych i związanych z nimi danych oraz do uznania ochrony tej infrastruktury krytycznej za element spoczywającego na nich obowiązku należytej staranności; apeluje do państw członkowskich o przyjęcie i wdrożenie strategii, wytycznych i instrumentów zapewniających uzasadnione poziomy ochrony przed rozsądnie identyfikowalnymi poziomami zagrożenia, przy czym koszty i obciążenia związane z ochroną powinny być proporcjonalne do możliwych szkód, na jakie narażone są zainteresowane strony; wzywa państwa członkowskie do podjęcia odpowiednich działań na rzecz zobligowania osób prawnych na obszarze ich jurysdykcji do ochrony powierzonych im danych osobowych;

62. uznaje fakt, że ze względu na zmieniające się środowisko cyberzagrożeń może być zalecana silniejsza i bardziej zorganizowana współpraca ze służbami policyjnymi, w szczególności w niektórych obszarach krytycznych, np. podczas śledzenia takich zagrożeń jak dżihad cybernetyczny, cyberterroryzm, radykalizacja w internecie i finansowanie organizacji ekstremistycznych lub radykalnych;

63. zachęca do ścisłej współpracy agencji UE, takich jak EDA, ENISA i Europejskie Centrum ds. Walki z Cyberprzestępczością, w ramach międzysektorowego podejścia mającego na celu promowanie synergii i unikanie powielania działań;

64. apeluje do Komisji o opracowanie planu działania dotyczącego skoordynowanego podejścia do europejskiej cyberobrony, w tym aktualizacji ram unijnej polityki w zakresie cyberobrony, by zagwarantować, że ramy te nadal będą stanowiły odpowiedni do zamierzonego celu instrument polityki ukierunkowany na osiągnięcie unijnych celów w zakresie cyberobrony, z zachowaniem ścisłej współpracy z państwami członkowskimi, EDA, Parlamentem oraz ESDZ; zauważa, że proces ten musi stanowić element szerszego podejścia strategicznego do WPBiO;

65. wzywa do budowania zdolności w obszarze cyberbezpieczeństwa w drodze współpracy na rzecz rozwoju oraz ciągłego kształcenia i szkolenia w dziedzinie świadomości cybernetycznej, z uwzględnieniem faktu, że w najbliższych latach miliony nowych użytkowników zaczną korzystać z dostępu do internetu, większość z nich w krajach rozwijających się, i w ten sposób zwiększenia odporności państw i społeczeństw na zagrożenia cybernetyczne i hybrydowe;

66. wzywa do nawiązania współpracy międzynarodowej i podjęcia wielostronnych inicjatyw na rzecz opracowania rygorystycznych ram cyberobrony i cyberbezpieczeństwa, aby przeciwdziałać zawłaszczaniu państwa w drodze korupcji, oszustwom finansowym, praniu pieniędzy, finansowaniu terroryzmu, oraz w celu stawienia czoła problemom związanym z cyberterroryzmem i kryptowalutami oraz innymi alternatywnymi metodami płatności;

67. zauważa, że w sytuacji braku rozległej odporności na całym świecie cyberataki takie jak NotPetya rozprzestrzeniają się szybko i powodują powszechne szkody; uważa, że szkolenie i kształcenie w dziedzinie cyberobrony powinno stanowić element działań zewnętrznych UE, a budowanie cyberodporności państw trzecich przyczynia się do osiągnięcia międzynarodowego pokoju i bezpieczeństwa, co ostatecznie zapewnia większe bezpieczeństwo europejskich obywateli;

Wzmocnienie instytucjonalne

68. wzywa państwa członkowskie do zaangażowania się w bardziej ambitną współpracę w sferze cyfrowej w ramach PESCO; sugeruje, aby państwa członkowskie uruchomiły nowy program współpracy cybernetycznej w ramach PESCO w celu wsparcia szybkiego i skutecznego planowania, dowodzenia i kontroli obecnych i przyszłych operacji i misji UE; zauważa, że powinno to prowadzić do lepszej koordynacji zdolności operacyjnych w cyberprzestrzeni i może skutkować opracowaniem wspólnego dowództwa w zakresie cyberobrony, jeżeli zdecyduje tak Rada Europejska;

69. ponawia swój apel do państw członkowskich oraz wiceprzewodniczącej Komisji / wysokiej przedstawiciel Unii ds. zagranicznych i polityki bezpieczeństwa o przedstawienie białej księgi UE w sprawie bezpieczeństwa i obrony; wzywa państwa członkowskie i wiceprzewodniczącą Komisji / wysoką przedstawiciel Unii ds. zagranicznych i polityki bezpieczeństw do umieszczenia cyberobrony i cyberprewencji u podstawy białej księgi, obejmującej zarówno ochronę domeny cybernetycznej dla operacji wskazanych w art. 43 TUE, jak i wspólną obronę, o której mowa w art. 42 ust. 7 TUE;

70. zauważa, że nowy program współpracy cybernetycznej w ramach PESCO powinien być kierowany przez personel wojskowy i cywilny wysokiego szczebla z każdego państwa członkowskiego, na zasadzie rotacji, i być rozliczany przez unijnych ministrów obrony w formacie PESCO oraz wiceprzewodniczącą Komisji / wysoką przedstawiciel Unii ds. zagranicznych i polityki bezpieczeństwa, w celu wsparcia zasady zaufania między państwami członkowskimi i instytucjami i agencjami UE przy wymianie informacji i danych wywiadowczych;

71. ponawia swój apel o stworzenie Rady Obrony UE w oparciu o obecną ministerialną Radę Sterującą EDA i format PESCO unijnych ministrów obrony, aby zagwarantować priorytetowe traktowanie, operacjonalizację zasobów i skuteczną współpracę i integrację między państwami członkowskimi;

72. przypomina o potrzebie zachowania Europejskiego Funduszu Obronnego lub nawet zwiększenia jego zasobów w kolejnych WRF, z przydzieleniem wystarczającego budżetu na cele cyberobrony;

73. wzywa do zwiększenia środków w celu modernizacji i usprawnienia cyberbezpieczeństwa i rozpowszechniania informacji wywiadowczych między ESDZ/Centrum Analiz Wywiadowczych Unii Europejskiej (INTCEN), Radą i Komisją;

Partnerstwo publiczno-prywatne

74. uznaje fakt, że przedsiębiorstwa prywatne odgrywają kluczową rolę w wykrywaniu i ograniczaniu incydentów w zakresie cyberbezpieczeństwa, przeciwdziałaniu im oraz reagowaniu na nie, nie tylko jako dostawcy technologii, ale także jako dostawcy usług nieinformatycznych;

75. uznaje rolę sektorów prywatnych w wykrywaniu i ograniczaniu incydentów w zakresie cyberbezpieczeństwa, przeciwdziałaniu im oraz reagowaniu na nie, a także ich rolę w pobudzaniu innowacji w dziedzinie cyberobrony, i w związku z tym wzywa do zacieśnienia współpracy z sektorem prywatnym w celu zapewnienia wspólnych informacji w zakresie wymogów UE i NATO oraz pomocy w wypracowaniu wspólnych rozwiązań;

76. apeluje do UE o dokonanie kompleksowego przeglądu oprogramowania, sprzętu i infrastruktury z zakresu technologii informacyjnych i komunikacyjnych wykorzystywanych przez instytucje w celu wyeliminowania potencjalnie niebezpiecznych programów i urządzeń oraz zakazu stosowania tych, które zostały potwierdzone jako szkodliwe, np. Kaspersky Lab;

o

o o

77. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie Europejskiej, Radzie, Komisji, wiceprzewodniczącej Komisji / wysokiej przedstawiciel Unii ds. zagranicznych i polityki bezpieczeństwa, agencjom UE w dziedzinie obrony i cyberbezpieczeństwa, Sekretarzowi Generalnemu NATO oraz parlamentom narodowym państw członkowskich UE.