Czwartek, 7 października 2021 r.

P9_TA(2021)0412

Stan zdolności cyberobronnych UE

Rezolucja Parlamentu Europejskiego z dnia 7 października 2021 r. w sprawie stanu zdolności cyberobronnych UE (2020/2256(INI))

(2022/C 132/09)

Parlament Europejski,

— uwzględniając Traktat o Unii Europejskiej (TUE) i 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 28 czerwca 2016 r. przez wysoką przedstawiciel Unii do spraw zagranicznych i polityki bezpieczeństwa oraz wiceprzewodniczącą Komisji (wysoka przedstawiciel / wiceprzewodnicząca Komisji),

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

— 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 ([1]),

— 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 i wysokiej przedstawiciel Unii do spraw zagranicznych i polityki bezpieczeństwa z 13 września 2017 r. pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej" (JOIN(2017)0450),

— uwzględniając wspólną deklarację o współpracy UE-NATO, podpisaną w lipcu 2018 r.,

— uwzględniając decyzję Rady (WPZiB) 2019/797 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim,

— uwzględniając konkluzje Rady z dnia 10 grudnia 2019 r. w sprawie dodatkowych działań na rzecz zwiększenia odporności i przeciwdziałania zagrożeniom hybrydowym,

— uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych (akt o cyberbezpieczeństwie) ([2]),

— uwzględniając konkluzje Rady z dnia 16 czerwca 2020 r. w sprawie działań zewnętrznych UE w zakresie przeciwdziałania terroryzmowi i brutalnemu ekstremizmowi oraz zwalczania tych zjawisk,

— uwzględniając konkluzje Rady i przedstawicieli rządów państw członkowskich zebranych w Radzie w sprawie ustanowienia umowy w zakresie cywilnego wymiaru WPBiO,

— uwzględniając decyzję Rady (WPZiB) 2020/1127 z dnia 30 lipca 2020 r. zmieniającą decyzję (WPZiB) 2019/797 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim ([3]),

([1]) Dz.U. L 194 z 19.7.2016, s. 1.
([2]) Dz.U. L 151 z 7.6.2019, s. 15.
([3]) Dz.U. L 246 z 30.7.2020, s. 12.

— uwzględniając decyzję Rady (WPZiB) 2020/1537 z dnia 22 października 2020 r. zmieniającą decyzję (WPZiB) 2019/797 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim ([4]),

— uwzględniając komunikat Komisji z dnia 24 lipca 2020 r. w sprawie strategii UE w zakresie unii bezpieczeństwa (COM(2020)0605),

— uwzględniając wspólny komunikat Komisji oraz wysokiego przedstawiciela Unii do spraw zagranicznych i polityki bezpieczeństwa z dnia 16 grudnia 2020 r. pt. „Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę" (JOIN (2020)0018),

— uwzględniając wniosek Komisji z dnia 16 grudnia 2020 r. dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 (COM(2020)0823),

— uwzględniając wniosek Komisji z 16 grudnia 2020 r. dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie odporności podmiotów krytycznych (COM(2020)0829),

— uwzględniając konkluzje Rady z 9 marca 2021 r. w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę,

— uwzględniając oświadczenie Rady Europejskiej z 25 marca 2021 r.,

— uwzględniając sprawozdanie Otwartej Grupy Roboczej z 10 marca 2021 r.,

— uwzględniając program działania ONZ na rzecz rozbrojenia – „Zabezpieczenie naszej wspólnej przyszłości",

— uwzględniając cele zrównoważonego rozwoju ONZ, w szczególności cel nr 16 zakładający promowanie pokojowych i integracyjnych społeczeństw z myślą o zrównoważonym rozwoju,

— uwzględniając przygotowany przez Europejski Trybunał Obrachunkowy przegląd nr 09/2019 w sprawie obronności europejskiej,

— uwzględniając swoją rezolucję z dnia 13 czerwca 2018 r. w sprawie cyberobrony ([5]),

— uwzględniając art. 54 Regulaminu,

— uwzględniając sprawozdanie Komisji Spraw Zagranicznych (A9-0234/2021),

A. mając na uwadze, że UE i jej państwa członkowskie muszą dalej rozwijać strategię w zakresie cyberbezpieczeństwa, wyznaczającą realistyczne, precyzyjne i ambitne cele oraz wyraźnie określającą politykę na płaszczyźnie wojskowej i cywilnej, a także tam, gdzie obie te płaszczyzny się pokrywają; mając na uwadze, że wszystkie instytucje Unii i państwa członkowskie UE muszą ściślej współpracować na wszystkich szczeblach, aby przygotować tę strategię, której głównym celem powinno być dalsze wzmacnianie odporności, a w rezultacie rozwijanie wspólnych, ale również lepszych, krajowych i solidnych zdolności cywilnych i wojskowych w zakresie cyberbezpieczeństwa oraz współpracy, aby móc reagować na trwałe wyzwania w dziedzinie bezpieczeństwa;

B. mając na uwadze, że UE podjęła zobowiązanie do stosowania obowiązującego prawa międzynarodowego w dziedzinie cyberprzestrzeni, a w szczególności Karty Narodów Zjednoczonych, w której wzywa się państwa do załatwiania sporów międzynarodowych przy pomocy pokojowych środków i do powstrzymywania się w stosunkach międzynarodowych od stosowania groźby lub użycia siły przeciwko nietykalności terytorium albo niepodległości politycznej któregokolwiek państwa, lub wszelkiego innego sposobu niezgodnego z zasadami ONZ;

C. mając na uwadze, że w ostatnich latach obserwujemy stały wzrost liczby szkodliwych cyberoperacji prowadzonych przez podmioty państwowe i niepaństwowe przeciwko UE i jej państwom członkowskim, które uwidoczniły słabe punkty sieci niezbędnych dla bezpieczeństwa europejskiego; mając na uwadze, że agresywne podmioty w cyberprzestrzeni są coraz bardziej różnorodne, coraz liczniejsze i stosują coraz bardziej zaawansowane metody; mając na uwadze, że ataki te wymagają pilnej poprawy skuteczności środków obrony oraz rozwoju europejskich zdolności w zakresie cyberbezpieczeństwa; mając na uwadze, że szkodliwe cyberataki mogą mieć miejsce w każdej chwili, a podmioty zarówno na szczeblu UE, jak i krajowym należy zachęcać do podejmowania niezbędnych działań mających na celu stałe utrzymanie skutecznej cyberobrony, nawet w czasach pokoju;

([4]) Dz.U. L 351 I z 22.10.2020, s. 5.
([5]) Dz.U. C 28 z 27.1.2020, s. 57.

D. mając na uwadze, że pandemia COVID-19 i wzrost zagrożeń dla cyberbezpieczeństwa pokazały konieczność przyjęcia porozumień międzynarodowych; mając na uwadze, że podczas pandemii COVID-19 znacznie nasiliły się cyberataki, mając też na uwadze, że UE i jej państwa członkowskie zaobserwowały zagrożenia cybernetyczne i szkodliwe działania w cyberprzestrzeni wymierzone w podstawowe podmioty gospodarcze, w tym ataki mające na celu zakłócenie funkcjonowania infrastruktury krytycznej, takiej jak energetyka, transport i opieka zdrowotna, a także znaczną ingerencję obcych państw w cyberprzestrzeń, co doprowadziło do zatarcia granicy między pokojem a wrogością; mając na uwadze, że w planie odbudowy dla Europy przewidziano dodatkowe inwestycje w cyberbezpieczeństwo;

E. mając na uwadze, że cyberprzestrzeń jest obecnie uznawana za domenę operacyjną; mając na uwadze, że zagrożenia dla cyberbezpieczeństwa mogą narażać na szwank działania wojskowe we wszystkich tradycyjnych domenach operacyjnych, mając też na uwadze, że tradycyjne domeny operacyjne są zależne od funkcjonowania cyberprzestrzeni, a nie odwrotnie; mając na uwadze, że konflikty mogą toczyć się we wszystkich przestrzeniach fizycznych (na lądzie, w powietrzu, na morzu i w przestrzeni kosmicznej) i wirtualnych (w cyberprzestrzeni), mogą być wzmacniane przez elementy wojny hybrydowej, takie jak kampanie dezinformacyjne z wykorzystaniem cyberprzestrzeni, wojny zastępcze, ofensywne i defensywne wykorzystanie zdolności cybernetycznych oraz ataki strategiczne na dostawców usług cyfrowych mające na celu zakłócenie funkcjonowania infrastruktury krytycznej, a także naszych instytucji demokratycznych, oraz mogą powodować znaczne szkody finansowe;

F. mając na uwadze, że Europejska Służba Działań Zewnętrznych (ESDZ), Komisja oraz Europejska Agencja Obrony (EDA) powinny wspierać państwa członkowskie w koordynowaniu i zwiększaniu wysiłków na rzecz zapewnienia zdolności i technologii w zakresie cyberobrony, zajmując się wszystkimi aspektami rozwoju zdolności, w tym doktryną, przywództwem, organizacją, personelem, szkoleniem, branżą, technologią, infrastrukturą, logistyką, interoperacyjnością i zasobami;

G. mając na uwadze, że w czasie opracowywania katalogu potrzeb (2017 r.), który jest stosowany do określania pełnego zakresu wymogów militarnych wspólnej polityki bezpieczeństwa i obrony (WPBiO) na podstawie przykładowych scenariuszy, potrzeba zdolności w obszarze cyberobrony została opatrzona wysokim priorytetem;

H. mając na uwadze, że pomyślne wykonanie misji i operacji UE w coraz większym stopniu zależy od nieprzerwanego dostępu do bezpiecznej cyberprzestrzeni, a tym samym wymaga odpornych zdolności cyberoperacyjnych;

I. mając na uwadze, że w ramach polityki UE w zakresie cyberobrony, zaktualizowanych w 2018 r., określono priorytety, takie jak rozwój zdolności w zakresie cyberobrony oraz ochronę sieci komunikacyjnych i informacyjnych WPBiO;

J. mając na uwadze, że w swoim orędziu o stanie Unii w 2021 r. przewodnicząca Komisji podkreśliła potrzebę stworzenia polityki UE w zakresie cyberobrony;

K. mając na uwadze, że coraz większe włączanie sztucznej inteligencji (AI) w zdolności cybernetyczne sił obronnych (systemy cyberfizyczne, w tym komunikacja i łącza danych między pojazdami w systemie sieciowym) może prowadzić do podatności na ataki w ramach wojny elektronicznej, takie jak zakłócanie, spoofing lub hakowanie;

L. mając na uwadze, że podniesienie poziomu cyberbezpieczeństwa i cyberobrony UE jest niezbędnym warunkiem powodzenia europejskich ambicji cyfrowych i geopolitycznych oraz przyczyniłoby się do zwiększenia odporności, dotrzymując kroku rosnącemu zaawansowaniu i zagrożeniu atakami cybernetycznymi; mając na uwadze, że UE o silnej kulturze cyberbezpieczeństwa i silnej technologii cyberbezpieczeństwa, co obejmuje też zdolność do identyfikowania i przypisywania szkodliwych działań w sposób terminowy i skuteczny oraz odpowiedniego reagowania, byłaby w stanie chronić swoich obywateli, a także bezpieczeństwo swoich państw członkowskich;

M. mając na uwadze, że międzynarodowe organizacje terrorystyczne poszerzyły swoją wiedzę specjalistyczną w zakresie cyberwojny i zwiększyły zakres jej stosowania, a osoby przeprowadzające cyberataki wykorzystują najnowszą technologię do wykrywania słabych punktów w systemach i urządzeniach oraz uczestnictwa w cyberatakach na dużą i wielką skalę;

N. mając na uwadze, że wraz z pojawieniem się zaawansowanych cybertechnologii sektory obrony i przestrzeni kosmicznej stanęły w obliczu bezprecedensowej konkurencji globalnej i kluczowych zmian technologicznych; mając na uwadze, że Europejski Trybunał Obrachunkowy wskazał luki w zdolnościach w obszarze technologii komunikacyjno-informacyjnych, cyberwojny i sztucznej inteligencji; mając na uwadze, że UE jest importerem netto produktów i usług z dziedziny cyberbezpieczeństwa, przez co naraża się na większe ryzyko zależności technologicznej i podatności na zagrożenia ze strony operatorów spoza UE; mając na uwadze, że zestaw wspólnych unijnych zdolności w zakresie sztucznej inteligencji powinien wypełnić luki techniczne i zadbać o to, aby państwa członkowskie bez odpowiedniej technologicznej i branżowej wiedzy specjalistycznej lub możliwości wdrożenia systemów sztucznej inteligencji w ministerstwach obrony nie pozostawały w tyle;

O. mając na uwadze, że skandal z oprogramowaniem szpiegowskim Pegasus wykazał, że szpiegowano dużą liczbę dziennikarzy, działaczy na rzecz praw człowieka, parlamentarzystów i innych obywateli UE; mając na uwadze, że różne podmioty państwowe, takie jak Rosja, Chiny czy Korea Północna, podejmują szkodliwą działalność cybernetyczną, aby osiągać cele polityczne, ekonomiczne i związane z bezpieczeństwem, a działalność ta obejmuje ataki na krytyczną infrastrukturę, cyberszpiegostwo i masową obserwację obywateli Unii, wspomaganie kampanii dezinformacyjnych, rozpowszechnianie złośliwego oprogramowania oraz ograniczanie dostępu do internetu i działania systemów IT; mając na uwadze, że takie działania są sprzeczne z prawem międzynarodowym, prawami człowieka, podstawowymi prawami UE i stanowią ich naruszenie, zagrażając demokracji, bezpieczeństwu, porządkowi publicznemu i strategicznej autonomii UE, w związku z czym usprawiedliwiają wspólną reakcję UE, taką jak działanie w ramach wspólnej unijnej reakcji dyplomatycznej, włącznie z użyciem sankcji przewidzianych w zestawie narzędzi dla unijnej cyberdyplomacji;

P. mając na uwadze, że 30 lipca 2020 r. Rada po raz pierwszy podjęła decyzję o nałożeniu środków ograniczających na osoby, podmioty i organy odpowiedzialne za różne cyberataki lub w nie zaangażowane, aby skuteczniej zapobiegać szkodliwym zachowaniom w cyberprzestrzeni, eliminować je i powstrzymywać oraz reagować na nie; mając na uwadze, że w maju 2019 r. przyjęto ramy prawne unijnych systemów sankcji związanych z cyberatakami;

Q. mając na uwadze, że formy przypisania cyberataków ich sprawcom stanowią centralny element cyberdyplomacji i strategii odstraszania;

R. mając na uwadze, że w ostatnich latach współpraca UE-NATO zacieśniła się w wielu dziedzinach, w tym w zakresie cyberbezpieczeństwa i cyberobrony zgodnie ze wspólną deklaracją UE-NATO z 2016 r.;

S. mając na uwadze, że sprawozdania konsensualne grupy ekspertów rządowych ONZ z lat 2010, 2013 i 2015, zatwierdzone przez Zgromadzenie Ogólne ONZ, stanowią uniwersalne ramy normatywne dla cyberstabilności, polegające na uznaniu, że obowiązujące prawo międzynarodowe, w tym Karta Narodów Zjednoczonych w całości, ma zastosowanie w cyberprzestrzeni, podobnie jak 11 dobrowolnych niewiążących norm odpowiedzialnego zachowania państw, a także działania zwiększające zaufanie oraz budowanie potencjału;

Stan zdolności cyberobronnych UE

1. podkreśla, że wspólna polityka cyberobrony i znacząca współpraca na szczeblu UE w zakresie tworzenia wspólnych, a także lepszych zdolności cyberobrony, są podstawowymi elementami rozwoju pogłębionej i wzmocnionej Europejskiej Unii Obrony i wymagają złożonego połączenia zdolności technicznych, strategicznych i operacyjnych; stwierdza, że cyberobrona odnosi się do działań, instrumentów i procesów, które są proporcjonalne i zgodne z prawem międzynarodowym, które obejmują zarówno elementy wojskowe, jak i cywilne, i które mają na celu ochronę m.in. sieci komunikacyjnych i informacyjnych WPBiO oraz misji i operacji WPBiO, a także pomoc państwom członkowskim; podkreśla pilną potrzebę rozwoju i wzmocnienia zarówno zdolności wspólnych, jak i zdolności państw członkowskich w zakresie cyberobrony na płaszczyźnie wojskowej;

2. przypomina, że ponadgraniczny charakter cyberprzestrzeni, a także znaczna liczba i coraz większa złożoność cyberataków wymagają skoordynowanej reakcji na szczeblu Unii, w tym wspólnych zdolności wsparcia państw członkowskich i pomocy państw członkowskich w odniesieniu do środków z zestawu narzędzi dla unijnej cyberdyplomacji, a także zacieśnionej współpracy UE-NATO opartej na wymianie informacji między zespołami reagowania kryzysowego w dziedzinie cyberbezpieczeństwa, wymianie najlepszych praktyk, zintensyfikowanych szkoleniach, badaniach i ćwiczeniach;

3. pochwala przegląd ram polityki UE w zakresie cyberobrony jako narzędzie wspomagania rozwoju zdolności państw członkowskich w obszarze cyberobrony; podkreśla, że przegląd ram polityki UE w zakresie cyberobrony powinien przede wszystkim skupić się na istniejących lukach i słabościach w unijnych i krajowych strukturach wojskowych; podkreśla potrzebę zwiększenia koordynacji między instytucjami, agencjami i organami UE, z państwami członkowskimi i między nimi, a także z Parlamentem Europejskim, aby zagwarantować, że zaktualizowane ramy polityki UE w zakresie cyberobrony osiągną cele cyberobronne UE;

4. wzywa ESDZ i Komisję do dalszego opracowywania, we współpracy z państwami członkowskimi, kompleksowego zestawu środków i spójnej polityki bezpieczeństwa informatycznego w celu zwiększenia odporności, ale także koordynacji wojskowej cyberobrony; wzywa do wzmocnienia współpracy z unijnym cywilnym zespołem reagowania na incydenty komputerowe (CERT-UE) w celu ochrony sieci wykorzystywanych przez wszystkie instytucje, organy i agencje UE, w ścisłej współpracy z dyrektorami ds. informatycznych w poszczególnych podmiotach, oraz do wzmocnienia komunikacji instytucji, organów i agencji UE z państwami członkowskimi; wzywa Parlament Europejski do zagwarantowania, że jego

udział w CERT-UE doprowadzi do zapewnienia takiego poziomu bezpieczeństwa informatycznego, który umożliwi mu otrzymywanie wszelkich niezbędnych informacji niejawnych i jawnych w celu wykonywania obowiązków wynikających z traktatów, w tym w wyniku obecnego procesu zastępowania porozumienia międzyinstytucjonalnego z 2002 r. w sprawie dostępu do informacji w dziedzinie bezpieczeństwa i obrony; wzywa ESDZ do zapewnienia odpowiedniego poziomu cyberbezpieczeństwa jej aktywów, pomieszczeń i działań, w tym siedziby, delegatur UE oraz misji i operacji WPBiO;

5. odnotowuje cel ram polityki w zakresie cyberobrony z 2018 r., jakim jest utworzenie wojskowej sieci CERT-UE; wzywa państwa członkowskie do znacznego zwiększenia zdolności wymiany informacji niejawnych, aby ułatwić wymianę informacji tam, gdzie jest ona potrzebna i użyteczna, oraz do opracowania szybkiej i bezpiecznej europejskiej sieci służącej do wykrywania i oceny cyberataków oraz przeciwdziałania im;

6. przypomina, że w priorytetach UE w zakresie rozwoju zdolności na 2018 r., określonych w planie rozwoju zdolności (CDP), zwrócono uwagę na potrzebę opracowania pełnego spektrum zdolności, a cyberobronę uznano za kluczowy priorytet; przypomina, że w priorytetach UE w zakresie rozwoju zdolności podkreślono, że technologie orientacji sytuacyjnej w cyberprzestrzeni i technologie cyberobrony mają kluczowe znaczenie w przeciwdziałaniu zagrożeniom dla bezpieczeństwa; z zadowoleniem przyjmuje wsparcie EDA dla państw członkowskich w rozwijaniu zdolności do poprawy cyberodporności, takich jak zdolność do wykrycia cyberataku, odparcia go i odbudowy po nim; przyjmuje do wiadomości różne działania podejmowane przez państwa członkowskie w ramach EDA, w tym projekt EDA zatytułowany „Cyber Defence Requirements Engineering" (CyDRE), w ramach którego należy opracować architekturę korporacyjną dla operacji w cyberprzestrzeni, w tym zakres, funkcje i wymogi, w oparciu o przepisy krajowe i unijne;

7. wzywa państwa członkowskie do zdefiniowania wspólnego standardu komunikacji, który mógłby być stosowany w odniesieniu do informacji niejawnych i jawnych, aby przyspieszyć działania i zapewnić bezpieczną sieć służącą do przeciwdziałania cyberatakom;

8. przyjmuje z zadowoleniem skoordynowany roczny przegląd w zakresie obronności (CARD), czyli pierwszy szczegółowy przegląd obronności na szczeblu UE, który jest jednym z kluczowych narzędzi wspierających ogólną spójność wydatków na obronność, planowanie obronne i współpracę w dziedzinie obrony państw członkowskich, a także powinien przyczynić się do promowania inwestycji w rozwój zdolności cyberobronnych;

9. z zadowoleniem przyjmuje postępy poczynione już w ramach europejskiego programu rozwoju przemysłu obronnego w postaci kilku istotnych projektów dotyczących wywiadu, bezpiecznej komunikacji i cyberobrony; z zadowoleniem przyjmuje w szczególności wezwanie do stworzenia łatwego do zastosowania i wzajemnie połączonego zestawu narzędzi cybernetycznych na potrzeby obrony oraz fakt, że EFO pomoże również wzmocnić odporność i poprawić gotowość, zdolność reagowania i współpracę w dziedzinie cyberbezpieczeństwa, pod warunkiem że taki priorytet zostanie ustalony podczas negocjowania odpowiednich programów prac EFO; podkreśla, że zdolność Europy do opracowywania projektów cyberobrony zależy od opanowania technologii, sprzętu, usług i danych oraz ich przetwarzania, a także od zaufanych przedsiębiorstw branżowych, i jednocześnie apeluje o pełne wdrożenie i egzekwowanie dyrektywy w sprawie zamówień w dziedzinie obronności ([6]); wzywa państwa członkowskie do wykorzystania EFO do wspólnego wypracowania zdolności cyberobronnych;

10. z zadowoleniem przyjmuje zacieśnienie współpracy między państwami członkowskimi w dziedzinie cyberobrony oraz dowodzenia, kontroli, łączności, komputerów, wywiadu, obserwacji i rozpoznania (C4ISR), a także postępy osiągnięte w ramach stałej współpracy strukturalnej (PESCO), w tym poprzez realizację konkretnych projektów, takich jak zespoły szybkiego reagowania w dziedzinie cyberbezpieczeństwa i projekt dotyczący wzajemnej pomocy w obszarze cyberbezpieczeństwa; przypomina, że EFO i PESCO oferują doskonałe środki rozwoju zdolności w zakresie cyberobrony i przyspieszenia inicjatyw w zakresie cyberbezpieczeństwa, np. poprzez platformę wymiany informacji o zagrożeniach cybernetycznych i reagowaniu na incydenty oraz centrum koordynacji domen cybernetycznych i informatycznych; wzywa wszystkie państwa członkowskie do zapewnienia spójności i położenia nacisku na cyberzdolności przy opracowywaniu strategicznego wspólnego podejścia do priorytetów; wzywa do wspierania badań i innowacji oraz wymiany wiedzy fachowej, aby wykorzystać pełen potencjał PESCO i EFO; z zadowoleniem przyjmuje decyzję Rady z dnia 5 listopada 2020 r. zezwalającą państwom trzecim na przyłączenie się do poszczególnych projektów PESCO w niektórych szczególnych przypadkach, biorąc pod uwagę, że mogą one wnieść wartość dodaną i zapewnić fachową wiedzę techniczną

([6]) Dyrektywa Parlamentu Europejskiego i Rady 2009/81/WE z dnia 13 lipca 2009 r. w sprawie koordynacji procedur udzielania niektórych zamówień na roboty budowlane, dostawy i usługi przez instytucje lub podmioty zamawiające w dziedzinach obronności i bezpieczeństwa (Dz.U. L 216 z 20.8.2009, s. 76).

oraz dodatkowe zdolności, a także pod warunkiem, że spełnią uzgodniony zestaw warunków politycznych, merytorycznych i prawnych; podkreśla, że w strategicznym interesie UE może leżeć – w wyjątkowych przypadkach – udział państw członkowskich i państw trzecich w projektach PESCO związanych z cyberbezpieczeństwem w celu wypełnienia bardziej ambitnych zobowiązań, na zasadzie faktycznej wzajemności;

11. podkreśla, że cyberobrona jest postrzegana jako zadanie operacyjne we wszystkich misjach WPBiO oraz że przed rozpoczęciem procesów planowania WPBiO należy wypracować, przetestować i wdrożyć cyberodporność i powiązane zdolności; przypomina, że pomyślne przeprowadzenie misji i operacji UE w coraz większym stopniu zależy od nieprzerwanego dostępu do bezpiecznej cyberprzestrzeni, a tym samym wymaga odpornych zdolności cyberoperacyjnych, a także adekwatnych reakcji na ataki wymierzone w obiekty, misje i operacje wojskowe; podkreśla, że zgodnie z umową w zakresie cywilnego wymiaru WPBiO, cywilna WPBiO musi być odporna na zagrożenia cybernetyczne i w stosownym przypadku wspierać państwa przyjmujące, w tym poprzez monitorowanie, mentoring i doradztwo; zaleca wykorzystanie opcji wspomagających budowanie cyberzdolności u naszych partnerów, np. rozszerzenie mandatu unijnych misji szkoleniowych, tak aby obejmowały one aspekty cyberobrony lub uruchomienie cybermisji cywilnych;

12. z zadowoleniem przyjmuje decyzję Rady z dnia 14 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim, które umożliwiają stosowanie ukierunkowanych środków ograniczających w celu powstrzymania cyberataków stanowiących zagrożenie dla UE lub jej państw członkowskich i reagowania na nie, w tym cyberataków na państwa trzecie lub organizacje międzynarodowe; z zadowoleniem przyjmuje nałożenie takich środków ograniczających w lipcu 2020 r. i październiku 2020 r., co stanowiło wiarygodny krok w kierunku wdrożenia zestawu narzędzi dla unijnej dyplomacji cyfrowej, w tym środków ograniczających, oraz wzmocnienia w UE postawy polegającej na cyberprewencji; wzywa do dalszego rozwoju i ścisłego egzekwowania systemu proporcjonalnych środków ograniczających w celu powstrzymania cyberataków, przy jednoczesnym poszanowaniu europejskiej wizji internetu, która zakłada istnienie jednej, otwartej, neutralnej, wolnej, bezpiecznej i niepodlegającej fragmentacji sieci;

13. przypomina – mając na uwadze podwójny charakter cybertechnologii – że zabezpieczone produkty i usługi cywilne mają kluczowe znaczenie dla sektora wojskowego i przyczyniają się do lepszej cyberobrony; przyjmuje w związku z tym z zadowoleniem prace prowadzone przez ENISA przy udziale państw członkowskich i zainteresowanych podmiotów, by dostarczyć UE systemy certyfikacji produktów, usług i procesów w zakresie ICT w celu podniesienia ogólnego poziomu cyberbezpieczeństwa na jednolitym rynku cyfrowym; podkreśla kluczową, pionierską rolę UE w opracowywaniu norm, które kształtują krajobraz cyberbezpieczeństwa, przyczyniają się do uczciwej konkurencji w UE i na arenie światowej oraz reagują na środki eksterytorialne i zagrożenia dla bezpieczeństwa ze strony państw trzecich; dostrzega również ważną rolę ENISA we wspieraniu inicjatyw badawczych i innych form współpracy mających na celu zwiększenie cyberbezpieczeństwa; podkreśla znaczenie inwestycji w zdolności w obszarze cyberobrony i cyberbezpieczeństwa w celu wzmocnienia odporności i strategicznych zdolności UE i państw członkowskich; podkreśla w tym względzie znaczenie programów „Cyfrowa Europa" i „Horyzont Europa", zwłaszcza jego klastra „Bezpieczeństwo cywilne na rzecz społeczeństwa"; zauważa znaczenie dostępności odpowiednich instrumentów finansowych w wieloletnich ramach finansowych na lata 2021–2027 (WRF), a także Instrumentu na rzecz Odbudowy i Zwiększania Odporności (RRF);

14. pochwala postępy niektórych państw członkowskich we wprowadzaniu dowodzenia w dziedzinie cyberbezpieczeństwa w strukturach wojskowych;

Wizja strategiczna – osiągnięcie odporności w zakresie cyberobrony

15. zauważa, że Strategiczny kompas wzmocni i ukierunkuje realizację ambicji UE w zakresie bezpieczeństwa i obrony oraz przełoży te ambicje na wymogi w zakresie zdolności, w tym priorytetowo w dziedzinie cyberobrony, zwiększając tym samym zdolność UE i państw członkowskich do wykrywania i przypisywania szkodliwych działań w cyberprzestrzeni, zapobiegania im, powstrzymywania ich, reagowania na nie i odbudowy po nich dzięki wzmocnieniu jej pozycji, świadomości sytuacyjnej, narzędzi, procedur i partnerstw;

16. nalega, aby Strategiczny kompas pogłębił kulturę strategiczną w dziedzinie cyberbezpieczeństwa i usunął wszystkie przypadki dublowania się zdolności i mandatów; podkreśla, że konieczne jest przezwyciężenie obecnej fragmentacji i złożoności ogólnej architektury cybernetycznej w UE, a także przygotowanie wspólnej wizji osiągnięcia bezpieczeństwa i stabilności w cyberprzestrzeni;

17. podkreśla, że fragmentacji tej towarzyszą poważne obawy dotyczące braku zasobów i personelu na szczeblu UE, co utrudnia realizację ambicji stworzenia jak najbezpieczniejszego środowiska cyfrowego, i w związku z tym podkreśla potrzebę zwiększenia zarówno zasobów, jak i personelu; wzywa wiceprzewodniczącego/wysokiego przedstawiciela lub państwa członkowskie do zwiększenia zasobów finansowych i zasobów ludzkich w obszarze obrony cybernetycznej, co

dotyczy w szczególności analityków wywiadu cybernetycznego i ekspertów w dziedzinie kryminalistyki cybernetycznej, oraz do ich szkolenia w zakresie podejmowania decyzji i kształtowania polityki, wdrażania polityki, reagowania na incydenty cybernetyczne i prowadzenia dochodzeń, w tym rozwijania umiejętności w dziedzinie cyberbezpieczeństwa, aby zwiększyć zdolność UE do charakteryzowania i przypisywania ataków cybernetycznych, a tym samym do zapewnienia w krótkim czasie odpowiedniej reakcji politycznej, cywilnej i wojskowej; wzywa do dalszego finansowania CERT-EU i Centrum Analiz Wywiadowczych UE (INTCEN) oraz do wspierania państw członkowskich w tworzeniu i wzmacnianiu centrów operacji bezpieczeństwa (SOC) w celu zbudowania sieci SOC w całej UE, która mogłaby zacieśnić współpracę cywilno-wojskową, tak aby w porę ostrzegać o incydentach związanych z cyberbezpieczeństwem;

18. zwraca uwagę, że udoskonalone szkolenie i kształcenie wojskowe w UE w dziedzinie cyberbezpieczeństwa mogłoby znacznie poprawić poziom zaufania między państwami członkowskimi, usprawnić standardowe procedury operacyjne, tworząc bardziej przejrzyste zasady, oraz poprawić ich egzekwowanie; zwraca uwagę w tym kontekście na ważne działania szkoleniowe podejmowane przez Europejskie Kolegium Bezpieczeństwa i Obrony (EKBiO) w obszarze cyberbezpieczeństwa i w związku z tym wyraża zadowolenie z utworzenia platformy kształcenia, szkolenia, oceny i ćwiczeń w zakresie cyberbezpieczeństwa (ETEE), której celem jest przeprowadzanie szkoleń z zakresu cyberbezpieczeństwa i cyberobrony wśród personelu cywilnego i wojskowego, a także wprowadzanie niezbędnych rozwiązań harmonizacyjnych i normalizacyjnych w szkoleniach powiązanych z cyberprzestrzenią; podkreśla, że EKBiO powinno w większym stopniu korzystać ze strukturalnego finansowania UE, aby móc wnieść bardziej znaczący wkład w działania mające na celu rozwijanie w UE umiejętności cyberobrony, zwłaszcza mając na uwadze większe zapotrzebowanie na najlepszych ekspertów w dziedzinie cyberprzestrzeni; wzywa państwa członkowskie do promowania partnerstw ze środowiskiem akademickim mających na celu wspieranie programów badawczo-rozwojowych w zakresie cyberbezpieczeństwa w celu opracowania nowych wspólnych technologii, narzędzi i umiejętności mających zastosowanie zarówno w sektorze cywilnym, jak i obronnym; podkreśla znaczenie kształcenia w procesie upowszechniania wiedzy w społeczeństwie oraz znaczenie poprawy zdolności obywateli, by mogli bronić się przed cyberatakami;

19. podkreśla potrzebę uwzględnienia kwestii związanych z płcią w unijnej polityce w dziedzinie cyberobrony, która powinna ambitnie niwelować różnice w traktowaniu kobiet i mężczyzn jako specjalistów w dziedzinie cyberobrony, zwłaszcza w ramach aktywnych strategii sprzyjających włączeniu oraz dostosowanych programów szkoleniowych dla kobiet;

20. przypomina, że cyberobrona ma wymiar zarówno wojskowy, jak i cywilny, a zatem wymaga ściślejszej współpracy, synergii i spójności między instrumentami; zaznacza, że najpierw należy przeanalizować i omówić problemy współpracy i koordynacji, a następnie również braki w zasobach kadrowych i technicznych, zarówno na szczeblu krajowym, jak i UE; stwierdza, że pomyślne wdrożenie zasobów wojskowych i cywilnych można osiągnąć tylko przez szkolenia i ćwiczenia z udziałem wszystkich odpowiednich zainteresowanych podmiotów; w tym względzie zwraca uwagę na ćwiczenia NATO „Locked Shields" jako należące do najlepszych przykładów testowania i udoskonalania zdolności w obszarze cyberobrony, zarówno cywilnej, jak i wojskowej; wzywa zatem wiceprzewodniczącego / wysokiego przedstawiciela i Komisję do opracowania zintegrowanego podejścia politycznego i wspierania synergii oraz ścisłej współpracy między siecią wojskowych zespołów CERT, CERT-UE i siecią CSIRT;

21. z zadowoleniem przyjmuje wspólny komunikat wiceprzewodniczącego / wysokiego przedstawiciela i Komisji zatytułowany „Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę", który ma na celu zwiększenie synergii i współpracy między działaniami dotyczącymi cyberprzestrzeni, a prowadzonymi w sferze cywilnej, obronnej i kosmicznej; uważa, że strategia ta stanowi kamień milowy we wzmacnianiu cyberodporności UE i państw członkowskich, a tym samym ugruntowuje przywództwo cyfrowe UE i jej zdolności strategiczne;

22. zaleca powołanie wspólnej jednostki ds. cyberprzestrzeni, aby zacieśnić współpracę w celu reagowania na brak wymiany informacji między instytucjami, organami i agencjami UE, dzięki czemu zapewni się bezpieczną i szybką sieć informacji oraz umożliwi pełne wykorzystanie istniejących struktur, zasobów i zdolności; zwraca uwagę na ważną rolę, jaką wspólna jednostka ds. cyberprzestrzeni mogłaby odegrać w chronieniu UE przed poważnymi cyberatakami transgranicznymi, na podstawie koncepcji międzysektorowej wymiany informacji; podkreśla znaczenie koordynacji, która pozwala unikać powielania struktur i odpowiedzialności na etapie opracowywania; w związku z tym z zadowoleniem przyjmuje zalecenie Komisji z 23 czerwca 2021 r., które przewiduje, że należy stworzyć specjalne interfejsy ze wspólną jednostką ds. cyberberprzestrzeni, aby umożliwić wymianę informacji ze społecznością zajmującą się obroną cybernetyczną, w szczególności poprzez przedstawicielstwo ESDZ; podkreśla też, że przedstawiciele odpowiednich projektów PESCO powinni wspierać wspólną jednostkę ds. cyberprzestrzeni, zwłaszcza w odniesieniu do orientacji sytuacyjnej i gotowości;

23. przypomina, że ze względu na ich często podwójne zastosowanie, poprawa zdolności do cyberobrony wymaga również cywilnej wiedzy specjalistycznej w zakresie bezpieczeństwa sieci i informacji; podkreśla, że rozprzestrzenianie gotowych systemów podwójnego zastosowania może wiązać się z wyzwaniami polegającymi na eksploatowaniu tych

systemów przez coraz większą liczbę państw oraz wrogie podmioty niepaństwowe; wzywa Komisję i państwa członkowskie do uruchomienia różnych kluczowych dźwigni, takich jak certyfikacja i nadzorowanie odpowiedzialności podmiotów prywatnych; podkreśla, że innowacje technologiczne są napędzane głównie przez przedsiębiorstwa prywatne, a zatem współpraca z sektorem prywatnym i zainteresowanymi podmiotami cywilnymi, w tym z branżami i podmiotami zaangażowanymi w zarządzanie infrastrukturą krytyczną, a także z MŚP, społeczeństwem obywatelskim, organizacjami i środowiskiem akademickim, ma kluczowe znaczenie i powinna zostać wzmocniona; przyjmuje do wiadomości proponowany przegląd dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych (NIS) oraz wniosek dotyczący dyrektywy w sprawie odporności podmiotów krytycznych, których celem jest ochrona infrastruktury krytycznej i zwiększenie bezpieczeństwa łańcucha dostaw oraz włączenie podmiotów objętych regulacją do ekosystemu cyfrowego; przypomina, że każde państwo członkowskie UE powinno opracować specjalną politykę zarządzania ryzykiem w łańcuchu dostaw na rzecz cyberbezpieczeństwa, a zwłaszcza rozwiązać kwestię zaufanych wykonawców; przypomina również, że dyrektywa NIS powinna respektować kompetencje państw członkowskich i odsyła do odpowiednich opinii Podkomisji Bezpieczeństwa i Obrony na temat obu ww. wniosków;

24. z zadowoleniem przyjmuje uruchomienie w dniu 29 września 2020 r. europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (CyCLONe), co jeszcze bardziej usprawniło terminową wymianę informacji i poprawiło orientację sytuacyjną dzięki zniwelowaniu różnicy między poziomem technicznym a poziomem politycznym w UE; zwraca uwagę, że skuteczne zdolności do cyberobrony wymagają zmiany kultury wymiany informacji przez odejście od zasady ograniczonego dostępu na rzecz zasady potrzebnej wymiany;

25. z zadowoleniem przyjmuje plan działania Komisji dotyczący synergii między sektorem cywilnym, obronnym i kosmicznym oraz przypomina o ścisłej współzależności tych trzech sektorów w zakresie cyberobrony; zauważa, że w odróżnieniu od innych dziedzin wojskowych infrastruktura wykorzystywana do „tworzenia" cyberprzestrzeni jest obsługiwana głównie przez podmioty komercyjne mające najczęściej siedzibę poza UE, co prowadzi do zależności przemysłowej i technologicznej od stron trzecich; jest głęboko przekonany, że UE musi zwiększyć swoją suwerenność technologiczną i pobudzać innowacyjność, inwestując w etyczne wykorzystanie nowych technologii w dziedzinie bezpieczeństwa i obrony, takich jak sztuczna inteligencja (AI) i obliczenia kwantowe; zachęca z całą mocą do opracowania ukierunkowanego na AI programu badań i rozwoju w państwach członkowskich; podkreśla jednak, że wojskowe wykorzystanie sztucznej inteligencji musi być zgodne z prawem międzynarodowym w dziedzinie praw człowieka oraz międzynarodowym prawem humanitarnym, a UE musi odgrywać przewodnią rolę w promowaniu globalnych ram regulacyjnych w dziedzinie sztucznej inteligencji, zakorzenionych w wartościach demokratycznych oraz opartych na zasadzie udziału czynnika ludzkiego;

26. odnotowuje wagę prac prowadzonych przez Centrum Satelitarne Unii Europejskiej i podkreśla, że Unia musi dysponować odpowiednimi zasobami w dziedzinie obserwacji satelitarnej i gromadzenia informacji wywiadowczych; zwraca się do tej agencji o przeanalizowanie i przedstawienie raportu dotyczącego bezpieczeństwa lub podatności satelitów UE i państw członkowskich na śmieci kosmiczne i cyberatak; zwraca uwagę, że Satcen powinno korzystać z większego finansowania strukturalnego UE, aby nadal móc wnosić wkład w działania Unii; podkreśla, że zdolności do cyberobrony mają kluczowe znaczenie dla zapewnienia bezpiecznej i odpornej wymiany informacji z SatCen zarówno w zakresie bezpieczeństwa z przestrzeni kosmicznej, jak i w przestrzeni kosmicznej, w celu zachowania i zwiększenia strategicznej autonomii UE w zakresie orientacji sytuacyjnej; podkreśla, że UE musi dążyć do zapobiegania uzbrojeniu przestrzeni kosmicznej;

27. z zadowoleniem przyjmuje decyzję Rady w sprawie ustanowienia Europejskiego Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa z siedzibą w Bukareszcie, które będzie przekazywać środki finansowe związane z cyberbezpieczeństwem pochodzące z programów „Horyzont Europa" i „Cyfrowa Europa", oraz zachęca do dobrej współpracy z siecią krajowych ośrodków koordynacyjnych; podkreśla znaczenie Centrum we wdrażaniu odpowiednich projektów i inicjatyw związanych z cyberbezpieczeństwem, które pomogą w osiągnięciu nowych zdolności będących podstawą odporności Unii, a także w usprawnieniu koordynacji między sektorem cywilnym i sektorem obrony w obszarze cyberbezpieczeństwa; podkreśla, że Centrum musi łączyć najważniejszych europejskich interesariuszy, w tym przedstawicieli przemysłu, organizacje akademickie i badawcze i inne odpowiednie stowarzyszenia społeczeństwa obywatelskiego, aby zwiększać i rozpowszechniać w całej UE fachową wiedzę z zakresu cyberbezpieczeństwa;

28. podkreśla znaczenie szyfrowania i legalnego dostępu do szyfrowanych danych; przypomina, że szyfrowanie danych oraz wzmocnienie i jak najszersze użycie takich zdolności może w istotny sposób przyczyniać się do cyberbezpieczeństwa państw, społeczeństw i przemysłu; wspiera program „europejskiej suwerenności cyfrowej" w celu propagowania i wzmocnienia aktualnych zdolności w obszarze narzędzi szyfrujących i poprawiających cyberbezpieczeństwo, inspirowany europejskimi podstawowymi prawami i wartościami, takimi jak prawo do prywatności, wolność wypowiedzi i demokracja, których celem jest umacnianie konkurencyjności europejskiej na rynku cyberbezpieczeństwa i pobudzanie popytu wewnętrznego;

29. z zadowoleniem przyjmuje zapowiadaną „wojskową wizję i strategię dotyczącą cyberprzestrzeni jako obszaru operacyjnego", która określi cyberprzestrzeń jako dziedzinę operacji w ramach WPBiO UE; wzywa do ciągłej oceny podatności infrastruktur informacyjnych misji WPBiO na zagrożenia oraz do wdrożenia wspólnych zharmonizowanych norm w zakresie kształcenia, szkolenia i ćwiczeń w dziedzinie cyberobrony w celu wsparcia misji WPBiO;

30. ubolewa nad faktem, że obecne ograniczenia obowiązujące w niejawnych systemach Komórek Planowania i Prowadzenia Operacji Wojskowych UE (MPCC) ograniczają jej możliwości; z tego względu wzywa Europejską Służbę Działań Zewnętrznych (ESDZ) do szybkiego zapewnienia MPCC najnowszego, anonimowego i bezpiecznego systemu teleinformatycznego (CIS), który będzie w stanie obsłużyć unijne dane niejawne na potrzeby misji i operacji WPBiO, z zachowaniem adekwatnego poziomu ochrony i odporności oraz z rozmieszczonym dowództwem sił;

31. wzywa do dalszego włączania cyberbezpieczeństwa do unijnych mechanizmów reagowania kryzysowego oraz do powiązania istniejących inicjatyw, struktur i procedur w różnych społecznościach cybernetycznych w celu zwiększenia wzajemnej pomocy i współpracy operacyjnej między państwami członkowskimi, w szczególności w przypadku poważnych cyberataków, aby zwiększyć interoperacyjność i wypracować wspólne rozumienie cyberobrony; zdecydowanie podkreśla znaczenie dalszych ćwiczeń, lecz przeprowadzanych z większą częstotliwością, i debat orientacyjnych opartych na różnych scenariuszach na temat zarządzania kryzysowego, w tym na temat klauzuli wzajemnej pomocy (art. 42 ust. 7 TUE) w hipotetycznym scenariuszu poważnego cyberataku, potencjalnie uznanego za atak zbrojny; apeluje, by takie inicjatywy wzmacniały wspólne zrozumienie procedur wykonawczych dotyczących wzajemnej pomocy lub solidarności zgodnie z art. 42 ust. 7 TUE i art. 222 TFUE, co obejmuje też szczególny cel zapewnienia gotowości tych procedur w odniesieniu do cyberataków na państwa członkowskie; z zadowoleniem przyjmuje komunikat ze szczytu NATO w Brukseli z 14 czerwca 2021 r., w którym potwierdzono zaangażowanie NATO w nieprzerwane wykorzystywanie pełnego zakresu zdolności w celu aktywnego powstrzymywania, obrony i przeciwdziałania pełnemu spektrum zagrożeń cybernetycznych, w tym decyzję o powołaniu się na art. 5 „w indywidualnych przypadkach"; wyraża zadowolenie z powodu dalszych dyskusji na temat powiązań między ramami zarządzania kryzysem cyberbezpieczeństwa w UE a narzędziami cyberdyplomacji;

32. zauważa, że UE jest w coraz większym stopniu zaangażowana w konflikty hybrydowe z przeciwnikami geopolitycznymi; podkreśla, że działania te są szczególnie destabilizujące i niebezpieczne, ponieważ zacierają granicę między wojną a pokojem, destabilizują systemy demokratyczne i sieją wątpliwości w umysłach ludności, w którą są wymierzone; przypomina, że chociaż tego rodzaju ataki same w sobie często nie są dostatecznie poważne, aby uruchomić art. 5 Traktatu Północnoatlantyckiego lub art. 42 ust. 7 TUE, to jednak mają skumulowane oddziaływanie strategiczne i nie można im skutecznie przeciwdziałać działaniami odwetowymi ze strony poszkodowanego państwa członkowskiego; uważa zatem, że UE powinna dążyć do przyjęcia rozwiązania, które pozwoli wypełnić tę próżnię prawną i dokonać ponownej interpretacji art. 42 ust. 7 TUE oraz art. 222 TFUE w taki sposób, aby zastrzec prawo do zbiorowej obrony w przypadkach, w których próg zbiorowej obrony nie zostanie osiągnięty, oraz umożliwić dobrowolne zbiorowe działania zaradcze państw członkowskich UE, a także powinna prowadzić współpracę międzynarodową z sojusznikami w celu wypracowania podobnego rozwiązania na szczeblu międzynarodowym; podkreśla, że jest to jedyny skuteczny sposób na powstrzymanie paraliżu w reagowaniu na zagrożenia hybrydowe, a także instrument zwiększający koszty po stronie naszych przeciwników;

33. ponownie podkreśla, że wspólne silne zdolności w zakresie przypisywania odpowiedzialności za atak są jednym z kluczowych narzędzi wzmacniania zdolności UE i państw członkowskich oraz stanowią zasadniczy element skutecznej cyberobrony i cyberprewencji; podkreśla, że usprawnienie wymiany informacji technicznych, analiz i informacji wywiadowczych o zagrożeniach między państwami członkowskimi na szczeblu UE mogłoby umożliwić zbiorcze przypisywanie odpowiedzialności na szczeblu UE; uznaje, że cyberobrona jest do pewnego stopnia skuteczniejsza, jeżeli obejmuje również pewne środki i działania ofensywne, pod warunkiem że ich stosowanie jest zgodne z prawem międzynarodowym; podkreśla, że bezpośrednie przypisanie cyberataków ich sprawcom jest skutecznym instrumentem odstraszającym; zachęca do rozważenia wspólnego publicznego przypisywania odpowiedzialności za szkodliwe działania w cyberprzestrzeni, w tym możliwości tworzenia sprawozdań o zachowaniach konkretnych podmiotów w cyberprzestrzeni, opracowywanych pod auspicjami ESDZ w formie podsumowania na szczeblu UE, dotyczących finansowanych przez państwa szkodliwych działań w cyberprzestrzeni wymierzonych w państwa członkowskie;

34. uważa współpracę cybernetyczną UE-NATO za kluczową, ponieważ mogłaby ona umożliwić i wzmocnić formalne wspólne przypisanie odpowiedzialności za wrogie cyberincydenty, a w konsekwencji nakładanie restrykcyjnych sankcji i środków; zauważa, że skuteczna odporność oraz skuteczny efekt odstraszający zostałyby osiągnięte, gdyby sprawcy znali katalog możliwych środków zaradczych, mieli świadomość ich proporcjonalności i stosowności oraz zgodności z prawem międzynarodowym, a w szczególności z Kartą ONZ (w zależności od stopnia nasilenia, skali i celu cyberataków);

35. pochwala propozycję wiceprzewodniczącego / wysokiego przedstawiciela zachęcającą do powołania grupy roboczej państw członkowskich UE ds. cyberwywiadu z siedzibą przy (INTCEN) oraz ułatwiającą utworzenie takiej grupy, aby zacieśnić strategiczną współpracę wywiadowczą dotyczącą zagrożeń dla cyberbezpieczeństwa i działań w cyberprzestrzeni,

a tym samym w dalszym ciągu wspierać orientację sytuacyjną UE oraz proces podejmowania decyzji w sprawach dotyczących wspólnych reakcji dyplomatycznych; zachęca do dalszych postępów w związku ze wspólnym zestawem propozycji, w szczególności jeśli chodzi o bieżącą interakcję z Komórką UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych oraz Komórką Analizy Zagrożeń Hybrydowych NATO w celu wymiany informacji w obszarze orientacji i analizy sytuacyjnej oraz w ramach współpracy taktycznej i operacyjnej;

Wzmacnianie partnerstw i zwiększanie roli UE w kontekście międzynarodowym

36. uważa, że współpraca z NATO w dziedzinie cyberobrony ma istotne znaczenie dla zapobiegania i przeciwdziałania cyberatakom w dziedzinach istotnych dla zbiorowego bezpieczeństwa państw członkowskich, a w stosownych przypadkach reagowania na takie ataki; wzywa państwa członkowskie do pełnego udostępnienia dowodów i informacji wywiadowczych na potrzeby utworzenia wykazu sankcji za cyberataki; wzywa do zwiększenia koordynacji tej kwestii z NATO poprzez udział w ćwiczeniach i wspólnych szkoleniach w dziedzinie cyberbezpieczeństwa, takich jak równoległe i skoordynowane ćwiczenia;

37. uznaje, że UE i NATO powinny koordynować działania w sytuacjach, w których wrogie podmioty zagrażają euroatlantyckim interesom w obszarze bezpieczeństwa; wyraża zaniepokojenie systemowym agresywnym zachowaniem w cyberprzestrzeni demonstrowanym zwłaszcza przez Chiny, Rosję i Koreę Północną, w tym licznymi atakami cybernetycznymi na instytucje rządowe i przedsiębiorstwa prywatne; uważa, że współpraca UE-NATO powinna koncentrować się na wyzwaniach w dziedzinie cyberbezpieczeństwa, technologii hybrydowych, nowo powstających i przełomowych technologii (EDT), przestrzeni kosmicznej, kontroli zbrojeń i nierozprzestrzeniania broni; wzywa do współpracy UE-NATO zapewniającej odporne, przystępne cenowo oraz bezpieczne i szybkie sieci zgodne z unijnymi i krajowymi standardami bezpieczeństwa, które zabezpieczają krajowe i międzynarodowe sieci informacyjne zdolne do szyfrowania wrażliwych danych i komunikacji;

38. z zadowoleniem przyjmuje porozumienie między CERT-UE a komórką NATO ds. reagowania na incydenty komputerowe (NCIRC), aby zapewnić zdolność do reagowania na zagrożenia w czasie rzeczywistym przez poprawę zapobiegania cyberincydentom, wykrywanie ich i reagowanie na nie zarówno w UE, jak i w NATO; podkreśla również znaczenie zwiększenia możliwości szkoleniowych w zakresie cyberobrony w systemach informatycznych i cybernetycznych we współpracy z Centrum Doskonałości ds. Współpracy w Dziedzinie Obrony przed Atakami Cybernetycznymi (CCDCOE) oraz Akademią Komunikacji i Informacji NATO (NCI);

39. wzywa do dalszej współpracy UE-NATO, w szczególności w zakresie wymogów interoperacyjności cyberobrony, poprzez poszukiwanie możliwej komplementarności i wzajemnie korzystnego wzmocnienia potencjału, dążenie do połączenia odpowiednich struktur WPBiO i sfederalizowanej sieci misyjnej NATO, unikanie powielania działań oraz uznanie swoich odpowiednich obowiązków; wzywa do wzmocnienia unijnego narzędzia PESCO oraz inicjatyw NATO – inteligentnej obrony, inicjatywy sił połączonych i deklaracji w sprawie inwestycji w obronność – a także do promowania pozyskiwania i wykorzystywania, w celu lepszego wykorzystania synergii i efektywności w relacjach między dostawcami a użytkownikami końcowymi; z zadowoleniem przyjmuje postępy we współpracy między UE a NATO w obszarze cyberobrony, zwłaszcza dotyczącej wymiany koncepcji i doktryn, wzajemnego udziału w ćwiczeniach z zakresu cyberobrony oraz wzajemnych spotkań informacyjnych dotyczących w szczególności zarządzania kryzysem w kontekście cyberbezpieczeństwa; proponuje utworzenie wspólnego dla UE i NATO ośrodka informacji o zagrożeniach dla cyberbezpieczeństwa, a także wspólnej grupy zadaniowej ds. cyberbezpieczeństwa;

40. wzywa do ściślejszej koordynacji w zakresie cyberobrony między państwami członkowskimi, instytucjami UE, sojusznikami z NATO, ONZ i Organizacją Bezpieczeństwa i Współpracy w Europie (OBWE); zachęca w związku z tym do dalszego promowania środków budowy zaufania OBWE w cyberprzestrzeni i podkreśla potrzebę opracowania skutecznych narzędzi współpracy międzynarodowej w celu wspierania budowania potencjału cybernetycznego partnerów, a także opracowania i promowania środków budowy zaufania oraz integracyjnej współpracy ze społeczeństwem obywatelskim i zainteresowanymi stronami; przyjmuje z zadowoleniem duże znaczenie, jakie przypisano globalnej, otwartej, stabilnej i bezpiecznej cyberprzestrzeni w unijnej strategii współpracy w regionie Indo-Pacyfiku z dnia 19 kwietnia 2021 r.; wzywa do aktywnego zacieśniania więzi z mającymi podobne zapatrywania demokracjami w regionie Indo-Pacyfiku, takimi jak USA, Korea Południowa, Japonia, Indie, Australia i Tajwan, aby wymieniać się wiedzą i doświadczeniem oraz informacjami o zwalczaniu zagrożeń dla cyberbezpieczeństwa; podkreśla też znaczenie współpracy z innymi krajami, zwłaszcza w bezpośrednim sąsiedztwie UE, aby pomóc w budowaniu ich zdolności do obrony przed zagrożeniami dla cyberbezpieczeństwa; pochwala fakt, że Komisja wspiera programy na rzecz cyberbezpieczeństwa w Bałkanach Zachodnich oraz krajach Partnerstwa Wschodniego; podkreśla pilną potrzebę przestrzegania prawa międzynarodowego, w tym całej Karty Narodów Zjednoczonych, oraz stosowania się do powszechnie uznanych międzynarodowych ram normatywnych dotyczących odpowiedzialnego zachowania państw w cyberprzestrzeni i wkładu w trwające rozmowy na temat zasad stosowania prawa międzynarodowego w cyberprzestrzeni w kontekście ONZ;

41. podkreśla znaczenie trwałego partnerstwa w dziedzinie cyberbezpieczeństwa ze Zjednoczonym Królestwem, które należy do państw o największym arsenale cyberobronnym; wzywa Komisję do zbadania możliwości ponownego uruchomienia procesu mającego na celu określenie formalnych i uporządkowanych ram przyszłej współpracy w tej dziedzinie;

42. podkreśla potrzebę zapewnienia pokoju i stabilności w cyberprzestrzeni; wzywa wszystkie państwa członkowskie i UE, by w trakcie dyskusji i inicjatyw pod auspicjami ONZ – w tym poprzez zaproponowanie programu działań – wykazały się inicjatywą, by przyjęły proaktywne podejście do ustanowienia wspólnych dla całej UE ram regulacyjnych oraz by przyczyniły się do rzeczywistego zwiększenia odpowiedzialności, przestrzegania nowych norm i zapobiegania niewłaściwemu wykorzystywaniu technologii cyfrowych, a także do promowania odpowiedzialnego zachowania państw w cyberprzestrzeni, w oparciu o sprawozdania konsensualne grupy ekspertów rządowych ONZ zatwierdzone przez Zgromadzenie Ogólne ONZ; z zadowoleniem przyjmuje zalecenia zawarte w sprawozdaniu końcowym otwartej grupy roboczej, zwłaszcza w sprawie ustanowienia programu działania; zachęca ONZ do wspierania dialogu państw, naukowców, przedstawicieli środowiska akademickiego, organizacji społeczeństwa obywatelskiego, organizacji humanitarnych i sektora prywatnego, aby zapewniać integracyjne procesy kształtowania polityki w obszarze nowych przepisów międzynarodowych; domaga się przyspieszenia wszystkich podejmowanych obecnie wielostronnych wysiłków, aby rozwój technologiczny i nowe metody prowadzenia działań wojennych nie wyprzedziły rozwoju ram normatywnych i regulacyjnych; wzywa do modernizacji architektury kontroli zbrojeń, aby uniknąć powstania cyfrowej szarej strefy; wzywa do wzmocnienia misji pokojowych ONZ w zakresie zdolności do cyberobrony, zgodnie ze skuteczną realizacją ich mandatów;

43. przypomina swoje stanowisko w sprawie zakazu rozwoju, produkcji i stosowania w pełni autonomicznej broni umożliwiającej przeprowadzanie uderzeń bez merytorycznej interwencji człowieka; wzywa wiceprzewodniczącego / wysokiego przedstawiciela Komisji, państwa członkowskie i Radę Europejską do przyjęcia wspólnego stanowiska w sprawie autonomicznych systemów uzbrojenia, które zapewni merytoryczną kontrolę człowieka nad funkcjami krytycznymi takich systemów uzbrojenia; domaga się otwarcia międzynarodowych negocjacji w sprawie prawnie wiążącego instrumentu, który zakazałby w pełni autonomicznej broni;

44. podkreśla znaczenie współpracy z parlamentami narodowymi w celu wymiany najlepszych praktyk w obszarze cyberbezpieczeństwa;

o

o o

45. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie Europejskiej, Radzie, Komisji, wiceprzewodniczącemu Komisji / wysokiemu przedstawicielowi Unii ds. zagranicznych i polityki bezpieczeństwa, agencjom UE zaangażowanym w obronę i cyberbezpieczeństwo, sekretarzowi generalnemu NATO oraz rządom i parlamentom państw członkowskich.