HM Government

Y Strategaeth Seiber Genedlaethol 2022

Arloesi dyfodol seiber gyda'r DU gyfan

Y Strategaeth Seiber Genedlaethol 2022

Arloesi dyfodol seiber gyda'r DU gyfan

Cynnwys

Cynnwys ychwanegol

Rhagair

Mae'r Deyrnas Unedig yn gymdeithas agored a democrataidd, ac mae ei hanes o gydweithredu ac arloesi yn sail i'n llwyddiant fel cenedl fyd-eang sy'n edrych tuag allan. Gwelwn hyn yn ein hymateb i argyfyngau iechyd rhyngwladol ac wrth hyrwyddo targedau Sero Net. Ond mae manteision y dull hwn yn fwy amlwg yn y maes seiber nag yn unman arall.

Boed hynny'n wireddu'r manteision amrywiol y mae seiber yn eu cynnig i'n dinasyddion ac i'n heconomi wrth i ni godi'r gwastad ac uno'r wlad gyfan; gweithio gyda phartneriaid tuag at seiberofod sy'n adlewyrchu ein gwerthoedd cenedlaethol neu ddefnyddio ein gallu seiber yn llawn i ddylanwadu ar ddigwyddiadau byd-eang, mae'r DU yn gweld seiber fel ffordd o ddiogelu a hyrwyddo ein buddiannau mewn tirwedd sy'n cael ei hail-lunio gan dechnoleg.

Y Strategaeth Seiber Genedlaethol newydd yw ein cynllun i sicrhau bod y DU yn parhau i fod yn hyderus, yn fedrus ac yn gadarn yn y byd digidol hwn sy'n symud yn gyflym; a'n bod yn parhau i addasu, arloesi a buddsoddi er mwyn diogelu a hyrwyddo ein buddiannau mewn seiberofod.

Gan barhau o'r man mae Strategaeth Seiberddiogelwch Genedlaethol arloesol 2016 yn dod i ben, mae'r bennod nesaf hon yn ein harwain i ddyfodol lle mae'r DU hyd yn oed yn fwy cadarn yn erbyn ymosodiadau seiber. Fel y Gweinidog sy'n arwain ar hyn, rwyf yn glir ynghylch dau o'i nodau craidd: yn gyntaf dylem gryfhau'r technolegau sy'n hanfodol i seiber; yn ail, dylem gyfyngu ar ein dibyniaeth ar gyflenwyr neu dechnolegau unigol sy'n cael eu datblygu o dan gyfundrefnau nad ydynt yn rhannu ein gwerthoedd.

Gwyddoniaeth a thechnoleg y DU fydd canolbwynt y newid hwn, gan sicrhau bod seiber yn parhau i fod yn ased economaidd a strategol cenedlaethol, bod ein technoleg yn fwy dibynadwy a'i bod mewn sefyllfa well i amddiffyn yn erbyn sbectrwm o wrthwynebwyr seiber yr oedd eu galluoedd, tan yn ddiweddar, yn perthyn i wladwriaethau'n unig.

Fel llywodraeth, rydym wedi ymrwymo i wario £22 biliwn ar ymchwil a datblygu, ac i roi technoleg wrth galon ein cynlluniau ar gyfer diogelwch gwladol. Rydym i gyd wedi gweld potensial trawsnewidiol technolegau digidol ond hefyd, fel gyda 5G, eu potensial i amharu. Bydd ein cynlluniau ar gyfer deallusrwydd artiffisial a pholisi data yn helpu i sicrhau ein bod ar flaen y gad o ran y technolegau hyn, a bydd y camau a gymerir o dan y strategaeth seiber yn sicrhau bod gennym ffydd yn niogelwch a chadernid cyflenwyr a phartneriaid.

Mae creu'r Llu Seiber Cenedlaethol y llynedd yn gam sylweddol ymlaen yn ein gallu seiber ymosodol. Ond mae seiberddiogelwch sylfaenol yn dal yn ganolog i'n hymdrechion wrth i ni gryfhau ein hymateb i'r rheini sy'n ymosod ar y DU a'n dinasyddion. Rydym hefyd yn canolbwyntio ar wneud y sector cyhoeddus yn fwy cadarn, gan helpu cynghorau i ddiogelu eu systemau a data personol dinasyddion rhag meddalwedd wystlo ac ymosodiadau seiber eraill.

Fel cymdeithas, mae seiber yn rhywbeth i bawb. Drwy'r strategaeth hon, mae'r llywodraeth yn gwneud mwy i amddiffyn dinasyddion a chwmnïau'r DU, a'i phartneriaid rhyngwladol – gan helpu i wireddu ei gweledigaeth bod seiberofod yn lle dibynadwy a chadarn i bobl ac i fusnesau ffynnu.

Y Gwir Anrhydeddus Steve Barclay AS Canghellor Dugiaeth Caerhirfryn a Gweinidog Swyddfa'r Cabinet

Cyflwyniad

Cyfleoedd a heriau'r oes ddigidol

1. Mae datblygiadau amlwg mewn technoleg ynghyd â chostau is wedi gwneud y byd yn fwy cysylltiedig nag erioed o'r blaen, gan arwain at gyfleoedd, arloesedd a chynnydd anhygoel. Mae pandemig y coronafeirws (COVID-19) wedi cyflymu'r duedd hon, ond mae'n debyg mai megis dechrau mae'r newid strwythurol hirdymor hwn. Mae twf byd-eang seiberofod yn newid y ffordd rydym yn byw, yn gweithio ac yn cyfathrebu, ac yn trawsnewid y systemau hanfodol rydym yn dibynnu arnynt mewn meysydd fel cyllid, ynni, dosbarthu bwyd, gofal iechyd a thrafnidiaeth. Yn gryno, mae seiberofod bellach yn rhan annatod o'n diogelwch a'n ffyniant i'r dyfodol. Mae hyn yn cynnig cyfleoedd anhygoel i wledydd sydd wedi datblygu'n dechnolegol fel y DU fynd ar drywydd eu nodau cenedlaethol mewn ffyrdd newydd.

2. Mae graddfa a chyflymder y newid hwn – sy'n aml yn gyflymach na'n normau cymdeithasol, ein cyfreithiau a'n sefydliadau democrataidd – hefyd yn datgloi cymhlethdod, ansefydlogrwydd a risg nas gwelwyd o'r blaen. Yn ystod y flwyddyn ddiwethaf, gwelwyd ymosodiadau seiber ar ysbytai a phiblinellau olew, ysgolion a busnesau, gyda meddalwedd wystlo a meddalwedd ysbïo masnachol yn cael eu defnyddio i dargedu ymgyrchwyr, newyddiadurwyr a gwleidyddion. Mae natur drawswladol seiberofod yn golygu na ellir mynd i'r afael â'r heriau hyn heb gydweithio rhyngwladol, ond mae hefyd yn faes sy'n dod yn bwysicach o ran cystadleuaeth systemig a gwrthdaro rhwng buddiannau, gwerthoedd a gweledigaethau sy'n cystadlu â'i gilydd yn ein dyfodol byd-eang.

Ein gweledigaeth: pŵer seiber i gefnogi nodau cenedlaethol

3. Yn y cyd-destun hwn, mae pŵer seiber yn dod yn ffordd bwysicach byth o ddefnyddio pŵer cenedlaethol ac mae'n ffynhonnell o fantais strategol. **Mae pŵer seiber yn golygu'r gallu i ddiogelu ac i hyrwyddo buddiannau cenedlaethol mewn seiberofod a thrwyddo.** Bydd y gwledydd sydd yn y sefyllfa orau i lywio drwy gyfleoedd a heriau'r oes ddigidol yn fwy diogel, yn fwy cadarn ac yn fwy ffyniannus yn y dyfodol. Y DU yw un o'r gwledydd mwyaf digidol ddatblygedig yn y byd ac mae gan y llywodraeth hon agenda dechnoleg uchelgeisiol, gartref a thramor. Mae hyn yn golygu ein bod yn arbennig o agored i heriau seiberofod ond ein bod hefyd mewn sefyllfa unigryw i arwain y ffordd o ran manteisio ar ei gyfleoedd i'n dinasyddion ac er budd cyffredin dynoliaeth.

4. Dros y deng mlynedd nesaf, bydd y rhyngrwyd, technoleg ddigidol a'r seilwaith sy'n sail iddo yn dod yn fwy sylfaenol byth i'n buddiannau ni ac i rai ein cynghreiriaid a'n gwrthwynebwyr. Wrth i ni greu rôl newydd i'r DU mewn oes fwy cystadleuol, bydd cryfhau ein pŵer seiber yn ein galluogi i arwain y ffordd ar gyfer diwydiant a gwledydd eraill, bod ar flaen y gad o ran newidiadau mewn technoleg yn y dyfodol, lliniaru bygythiadau ac ennill mantais strategol dros ein gwrthwynebwyr a'n cystadleuwyr. Bydd yn gwneud y DU yn un o'r economïau digidol mwyaf diogel a deniadol i fyw, cynnal busnes a buddsoddi ynddi.

5. Ein gweledigaeth yw y bydd y **DU yn 2030 yn parhau i fod yn bŵer seiber cyfrifol a democrataidd blaenllaw, a fydd yn gallu diogelu a hyrwyddo ein buddiannau mewn seiberofod a thrwyddo i gefnogi nodau cenedlaethol**:

- cenedl fwy diogel a chadarn, wedi'i pharatoi'n well ar gyfer bygythiadau a risgiau sy'n esblygu a defnyddio ein galluoedd seiber i ddiogelu dinasyddion rhag troseddau, twyll a bygythiadau i'r wladwriaeth
- economi ddigidol arloesol a ffyniannus, gyda chyfle wedi'i rannu'n fwy cyfartal ar draws y wlad a'n poblogaeth amrywiol
- uwch-bŵer Gwyddoniaeth a Thechnoleg, sy'n harneisio technolegau trawsnewidiol yn ddiogel i gefnogi cymdeithas sy'n fwy gwyrdd ac yn iachach
- partner mwy dylanwadol a gwerthfawr ar y llwyfan byd-eang, gan siapio ffiniau dyfodol trefn ryngwladol agored a sefydlog ar yr un pryd â chynnal ein rhyddid i weithredu mewn seiberofod

6. Dros y degawd diwethaf, rydym wedi sefydlu'r DU fel pŵer seiber, gan adeiladu galluoedd gweithrediadau a seiberddiogelwch arloesol a sector seiberddiogelwch blaenllaw. Mae'r strategaeth hon yn adeiladu ar y cynnydd sylweddol a wnaed drwy Strategaeth Seiberddiogelwch Genedlaethol 2016-2021 a'r tri chasgliad pwysig a nodwyd yn Adolygiad Integredig y llywodraeth o Ddiogelwch, Amddiffyn, Datblygu a Pholisi Tramor. Yn gyntaf, yn yr oes ddigidol, bydd pŵer seiber y DU yn ffordd bwysicach fyth o gyflawni ein nodau cenedlaethol. Yn ail, mae cynnal ein pŵer seiber yn gofyn am strategaeth fwy cynhwysfawr ac integredig, gan ystyried ein hystod lawn o amcanion a galluoedd seiber. Ac yn drydydd, rhaid i hyn fod yn ddull gweithredu cymdeithas gyfan – bydd yr hyn sy'n digwydd yn ystafell y bwrdd neu'r ystafell ddosbarth yr un mor bwysig i'n seiberddiogelwch cenedlaethol â gweithredoedd arbenigwyr technegol a swyddogion y llywodraeth, a bydd gweithio mewn partneriaeth yn hanfodol i'n llwyddiant.


CHELTENHAM
Science
Festival
18.2 Cyber Skills a
@CyNam

Pum colofn ein strategaeth

7. Mae'r Adolygiad Integredig yn nodi pum 'cam blaenoriaeth' ar gyfer y strategaeth hon a byddwn yn defnyddio'r rhain fel colofnau ein fframwaith strategol, gan arwain a threfnu'r camau penodol y byddwn yn eu cymryd a'r canlyniadau y bwriadwn eu cyflawni erbyn 2025:

- **Colofn 1: Cryfhau ecosystem seiber y DU**, buddsoddi yn ein pobl a'n sgiliau a dyfnhau'r bartneriaeth rhwng llywodraeth, y byd academaidd a diwydiant
- **Colofn 2: Adeiladu DU ddigidol gydnerth a ffyniannus**, lleihau risgiau seiber er mwyn i fusnesau allu cynyddu manteision economaidd technoleg ddigidol a bod dinasyddion yn fwy diogel ar-lein ac yn hyderus bod eu data'n cael ei ddiogelu
- **Colofn 3: Cymryd yr awenau gyda'r technolegau sy'n hanfodol i bŵer seiber,** adeiladu ein gallu diwydiannol a datblygu fframweithiau i ddiogelu technolegau'r dyfodol
- **Colofn 4: Hyrwyddo arweinyddiaeth a dylanwad byd-eang yn y DU ar gyfer trefn ryngwladol sy'n fwy diogel, ffyniannus ac agored**, gan weithio gyda phartneriaid mewn llywodraeth a diwydiant a rhannu arbenigedd sy'n sail i bŵer seiber y DU
- **Colofn 5: Canfod, atal ac amharu ar ein gwrthwynebwyr er mwyn gwella diogelwch y DU mewn seiberofod a thrwyddo**, defnyddio sbectrwm llawn ysgogiadau'r DU mewn ffordd sy'n fwy integredig, creadigol a rheolaidd

8. Mae Rhan 1 y ddogfen hon yn nodi'r cyd-destun strategol rydym yn gweithredu ynddo, nodau ein strategaeth, a'r dull gweithredu strategol y byddwn yn ei fabwysiadu dros y degawd nesaf. Mae Rhan 2 yn nodi'r camau penodol y byddwn yn eu cymryd i gyflawni ein nodau hyd at 2025, wedi'u trefnu o dan y pum colofn hyn.

Gweledigaeth

Yn 2030 bydd y DU yn parhau i fod yn bŵer seiber cyfrifol a democrataidd blaenllaw, a fydd yn gallu diogelu a hyrwyddo ein buddiannau mewn seiberofod a thrwyddo i gefnogi nodau cenedlaethol.

Colofnau ac amcanion

Colofn 1

Cryfhau ecosystem seiber y DU

1. Cryfhau'r strwythurau, y partneriaethau a'r rhwydweithiau sy'n angenrheidiol i gefnogi dull gweithredu cymdeithas gyfan yng nghyswllt seiber.
2. Gwella ac ehangu sgiliau seiber y genedl ar bob lefel, gan gynnwys drwy broffesiwn seiber amrywiol o safon fyd-eang sy'n ysbrydoli ac yn arfogi talent ar gyfer y dyfodol.
3. Meithrin twf sector seiberddiogelwch a diogelwch gwybodaeth cynaliadwy, arloesol a chystadleuol yn rhyngwladol, gan ddarparu cynnyrch a gwasanaethau o safon, sy'n diwallu anghenion y llywodraeth a'r economi ehangach.

Colofn 2

Adeiladu DU ddigidol gadarn a ffyniannus

1. Gwella dealltwriaeth o risg seiber er mwyn sbarduno gweithredu mwy effeithiol ar seiberddiogelwch a seibergadernid.
2. Atal a gwrthsefyll ymosodiadau seiber yn fwy effeithiol drwy wella'r gwaith o reoli risg seiber yn sefydliadau'r DU, a darparu mwy o amddiffyniad i ddinasyddion.
3. Cryfhau cadernid ar lefel genedlaethol a sefydliadol er mwyn paratoi ar gyfer ymosodiadau seiber, ymateb iddynt ac adfer ar eu hôl.

Colofn 3

Cymryd yr awenau gyda'r technolegau sy'n hanfodol i seiberddiogelwch

1. Gwella ein gallu i ragweld, asesu a gweithredu ar y datblygiadau gwyddoniaeth a thechnoleg sydd bwysicaf i'n pŵer seiber.
2. Meithrin a chynnal mantais sofran a chysylltiedig o ran diogelwch technolegau sy'n hanfodol i seiberofod.
3. Sicrhau'r genhedlaeth nesaf o dechnolegau a seilwaith cysylltiedig, gan liniaru risgiau seiberddiogelwch dibyniaeth ar farchnadoedd byd-eang a sicrhau bod gan ddefnyddwyr y DU fynediad at gyflenwad amrywiol a dibynadwy.
4. Gweithio gyda'r gymuned sy'n cynnwys nifer o randdeiliaid i siapio'r gwaith o ddatblygu safonau technegol digidol byd-eang yn y meysydd blaenoriaeth sydd bwysicaf ar gyfer cynnal ein gwerthoedd democrataidd, sicrhau ein seiberddiogelwch, a hyrwyddo mantais strategol y DU drwy wyddoniaeth a thechnoleg.

2a. Cadw menter Crypt-Allwedd genedlaethol gadarn sy'n diwallu anghenion cwsmeriaid, partneriaid a chynghreiriaid Llywodraeth Ei Mawrhydi, ac sydd wedi lliniaru ein risgiau mwyaf sylweddol yn briodol, gan gynnwys y bygythiad gan ein gwrthwynebwyr mwyaf galluog

Colofn 4

Hyrwyddo arweinyddiaeth a dylanwad byd-eang y DU

1. Cryfhau seiberddiogelwch a seibergadernid partneriaid rhyngwladol a chynyddu gweithredu ar y cyd i amharu ar a rhwystro gwrthwynebwyr.
2. Llunio trefn lywodraethu fyd-eang i hyrwyddo seiberofod agored, heddychlon a diogel am ddim.
3. Ysgogi ac allforio arbenigedd a galluoedd seiber y DU i roi hwb i'n mantais strategol a hyrwyddo ein buddiannau ehangach o ran polisi tramor a ffyniant.

Colofn 5

Canfod, rhwystro ac amharu ar wrthwynebwyr

1. Canfod, archwilio a rhannu gwybodaeth am weithredwyr a gweithgareddau seiber maleisus sy'n gysylltiedig â gweithredwyr gwladwriaethol, troseddol a rhai maleisus eraill er mwyn amddiffyn y DU, ei buddiannau a'i dinasyddion.
2. Atal ac amharu ar weithgarwch a gweithredwyr seiber troseddol, gwladwriaethol a maleisus eraill yn erbyn y DU, ei buddiannau a'i dinasyddion.
3. Gweithredu mewn seiberofod a drwyddo i gefnogi ein diogelwch gwladol ac atal a chanfod troseddau difrifol.

Cefnogi nodau cenedlaethol

- Diogelwch a chadernid
- Uwch-bŵer Gwyddoniaeth a Thechnoleg
- Ffyniant economaidd
- Siapio'r drefn ryngwladol

Rhan 1:
Strategaeth

Cyd-destun Strategol

Prydain Fyd-eang mewn Oes Gystadleuol

9. Mae'r Adolygiad Integredig o Ddiogelwch, Amddiffyn, Datblygu a Pholisi Tramor, a gyhoeddwyd ym mis Mawrth 2021, yn disgrifio gweledigaeth y llywodraeth ar gyfer rôl y DU yn y byd dros y degawd nesaf a'r camau y byddwn yn eu cymryd hyd at 2025. Er mwyn i'r DU fod mewn gwell sefyllfa ar gyfer byd mwy cystadleuol, mae'n cydnabod bod yn rhaid i ni groesawu arloesedd ym maes gwyddoniaeth a thechnoleg er mwyn rhoi hwb i'n ffyniant cenedlaethol a'n mantais strategol. Mae'r Strategaeth Seiber Genedlaethol yn adeiladu ar y dull gweithredu hwn ac mae ei chyhoeddi yn un o'r ymrwymiadau o dan amcan strategol yr Adolygiad Integredig ar gyfer 'cynnal mantais strategol drwy wyddoniaeth a thechnoleg'.

Y dirwedd seiber

10. Nid yw'r heriau polisi a gyflwynir gan seiberofod yn rhai technolegol yn unig. Mae'r parth seiber yn amgylchedd sydd wedi cael ei greu gan bobl ac yn y bôn mae'n cael ei siapio gan ymddygiad pobl. Mae'n chwyddo ymddygiadau o'r fath er gwell neu er gwaeth, ac fel rheol bydd effeithiau hynny'n cael eu teimlo yn y byd ffisegol hefyd. Cwmnïau preifat, llywodraethau, sefydliadau nid-er-elw, dinasyddion unigol a hyd yn oed troseddwyr sy'n berchen ar seiberofod ac sy'n ei weithredu. Mae hyn yn golygu bod yn rhaid i unrhyw ymateb strategol i'r cyd-destun hwn gysylltu geostrategaeth a diogelwch gwladol, cyfiawnder troseddol a rheoleiddio sifil, polisïau economaidd a diwydiannol ac mae angen dealltwriaeth ddofn o'r gwahanol gyd-destunau diwylliannol neu gymdeithasol a'r systemau gwerthoedd sy'n rhyngweithio ar-lein.

11. Mae seiberofod hefyd yn croesi ffiniau cenedlaethol. Mae cadwyni cyflenwi technoleg a dibyniaethau hanfodol yn dod yn fwyfwy byd-eang, mae seiberdroseddwyr a gweithredwyr gwladwriaethol yn gweithredu o bob cwr o'r byd, mae cwmnïau technoleg pwerus yn allforio cynnyrch ac yn gosod eu safonau, ac mae'r rheolau a'r normau sy'n llywodraethu seiberofod a'r rhyngrwyd yn cael eu pennu mewn fforymau rhyngwladol. Mae seiberofod hefyd yn esblygu'n barhaus wrth i dechnoleg a'r ffordd mae pobl yn ei defnyddio newid, sy'n golygu ei bod yn rhaid i ni fabwysiadu dull gweithredu hyblyg ac ymatebol.

Haenau Seiberofod

Beth yw seiberofod?

I lawer ohonom, seiberofod yw'r byd rhithwir rydyn ni'n ei brofi pan fyddwn ni'n mynd ar-lein i gyfathrebu, gweithio a chyflawni tasgau bob dydd. Mewn termau technegol, mae seiberofod yn rhwydwaith rhyngddibynnol o dechnoleg gwybodaeth sy'n cynnwys y rhyngrwyd, rhwydweithiau telegyfathrebu, systemau cyfrifiadurol a dyfeisiau sydd wedi'u cysylltu â'r rhyngrwyd. I'r fyddin, ac wrth ystyried ein hymdrechion i wrthsefyll bygythiadau mewn seiberofod, mae'n barth gweithredol, ochr yn ochr â thir, môr, yr awyr a'r gofod.

Beth yw'r profiad o seiberofod? Yn ôl ei ddiffiniad, mae seiberofod yn ofod 'a rennir' ac mae ei faint a'i gymhlethdod yn golygu bod profiad pob unigolyn ohono'n unigryw. Mae dinasyddion yn cael mynediad at seiberofod pan fyddant yn edrych ar eu cyfrifon banc ar-lein neu'n ffrydio ffilm gartref. Mae busnesau'n defnyddio seiberofod i gysylltu eu staff â'r adnoddau sydd eu hangen arnynt, boed hynny'n fynediad at wybodaeth neu reolaeth dros broses weithgynhyrchu. Mae llywodraethau'n darparu gwasanaethau cyhoeddus i'w dinasyddion drwy ddefnyddio pyrth ar-lein. Mae gweithwyr seiber proffesiynol yn edrych 'o dan y bonet' ar y dechnoleg, y safonau a'r protocolau sy'n gwneud i'r cyfan 'weithio' i ddefnyddwyr. Mae'r holl grwpiau hyn yn defnyddio seiberofod mewn ffyrdd gwahanol ac at ddibenion gwahanol, ac rydym i gyd yn defnyddio mwy a mwy ohono.

Profiad ar-lein

- Cyfrifon e-bost
- Proffiliau chwarae gemau
- Cyfrif cyfryngau cymdeithasol
- Mewngofnodi i gyfrifon banc
- Cerdyn adnabod teithio digyswllt
- Proffil tracio ffitrwydd

Meddalwedd, systemau a data

- Systemau TG cwmnïau
- Cronfeydd data, ee cofnodion treth CThEM
- Systemau rheoli diwydiannol
- Windows/system weithredu
- Apiau ee WhatsApp, Facebook, TikTok
- Ieithoedd rhaglennu, Python, C++

Dyfeisiau ffisegol a chyfathrebu

- Llwybryddion, Hybiau
- Gweinyddion
- WiFi, Ether-rwyd
- Antenas Radio
- Oergelloedd clyfar
- Darllenwyr cardiau teithio digyswllt
- Ffonau, cyfrifiaduron personol a dyfeisiau personol eraill

Mae modd disgrifio seiberofod mewn tair haen:

Rhithwir

Y rhan o seiberofod y mae'r rhan fwyaf o bobl yn ei phrofi. Mae'n cynnwys cynrychiolaeth o bobl a sefydliadau drwy hunaniaeth rithiol mewn gofod rhithiol a rennir. Gallai cynrychiolaeth rithiol fod yn gyfeiriad e-bost, enw defnyddiwr, cyfrif cyfryngau cymdeithasol neu enw arall. Mae modd i un person neu un sefydliad gael mwy nag un hunaniaeth ar-lein. Ar y llaw arall, gallai nifer o bobl neu sefydliadau greu dim ond un hunaniaeth a rennir hefyd.

Rhesymegol

Y rhan o seiberofod sy'n cynnwys cod neu ddata, fel systemau gweithredu, protocolau, rhaglenni a meddalwedd arall. Does dim modd i'r haen resymegol weithio heb yr haen ffisegol ac mae gwybodaeth yn llifo drwy rwydweithiau wedi'u gwifro neu'r sbectrwm electromagnetig. Mae'r haen resymegol, ynghyd â'r haen ffisegol, yn caniatáu i hunaniaethau rhithwir gyfathrebu a gweithredu.

Ffisegol

Mae haen ffisegol seiberofod yn cynnwys yr holl galedwedd y mae data'n cael ei drosglwyddo arno, o'r llwybryddion, y gwifrau a'r hybiau sydd gennych yn eich cartref, i systemau telathrebu cymhleth mawr sy'n cael eu gweithredu gan gwmnïau technoleg mawr. Yn ogystal â seilwaith ffisegol, mae'n cynnwys y sbectrwm electromagnetig y caiff data ei drosglwyddo arno, fel WiFi a radio.

Pŵer seiber

12. Wrth galon ein strategaeth mae'r cysyniad o bŵer seiber, sy'n cael ei ddiffinio gennym fel gallu gwladwriaeth i ddiogelu ac i hyrwyddo ei buddiannau mewn seiberofod a thrwyddo. Rydym yn nodi pum dimensiwn eang o bŵer seiber sy'n cyd-fynd â cholofnau'r strategaeth hon:

- Y bobl, yr wybodaeth, y sgiliau, y strwythurau a'r partneriaethau sy'n sail i'n pŵer seiber, sy'n sail i'r holl gydrannau eraill ac yn eu hintegreiddio mewn dull gweithredu cenedlaethol
- Y gallu i ddiogelu ein hasedau drwy seiberddiogelwch a seibergadernid, er mwyn gwireddu'r manteision llawn y mae seiberofod yn eu cynnig i'n dinasyddion ac i'n heconomi
- Y gallu technegol a diwydiannol i gynnal ein rhan yn natblygiad technolegau seiber allweddol a defnyddio datblygiadau newydd er budd cymdeithas
- Y dylanwad byd-eang, y perthnasoedd a'r safonau moesegol i siapio rheolau a normau mewn seiberofod yn unol â'n gwerthoedd a'n buddiannau a hyrwyddo diogelwch a sefydlogrwydd rhyngwladol
- Y gallu i weithredu mewn seiberofod a thrwyddo i gefnogi diogelwch cenedlaethol, lles economaidd ac atal troseddu. Mae hyn yn cynnwys gweithrediadau seiber i sicrhau effaith yn y byd go iawn, ac i helpu i sicrhau mantais strategol, a gweithrediadau gorfodi'r gyfraith a defnyddio sancsiynau seiber i ddod â seiberdroseddwyr maleisus o flaen eu gwell ac amharu ar eu gweithgareddau

13. Mae pŵer seiber yn wahanol i fathau mwy traddodiadol o bŵer. Mae'n golygu cyfuno galluoedd caled ac ysgogiadau dylanwadu meddalach yn ddi-dor. Mae ar fwy o wasgar ac mae'n rhaid i lywodraethau weithio gyda phartneriaid i'w ennill a'i ddefnyddio. Ac mae cyflymder y newid technolegol yn golygu bod modd ei ennill a'i golli'n gyflymach, gan fod galluoedd a oedd yn arfer bod rhai arloesol yn dod i ddiwedd eu hoes oherwydd datblygiadau newydd.

14. Mae ein strategaeth yn adlewyrchu hyn, gan ddisgrifio sut byddwn yn gweithio gyda phartneriaid lle bynnag y gallwn fel rhan o ymdrech cymdeithas gyfan. Byddwn yn gwneud mwy i fynd i'r afael â phroblemau uwch a datrys achosion gwaelodol, yn rhagweld tueddiadau yn y dyfodol ac yn rhoi ymatebion hirdymor ar waith, a byddwn yn fwy gweithredol o ran siapio yn hytrach nag ymateb i'r amgylchedd geowleidyddol sy'n cael ei herio.

Y DU fel pŵer seiber heddiw

15. Mae'r DU eisoes yn un o'r prif bwerau seiber.[1] Dros y degawd diwethaf, mae'r llywodraeth wedi arwain ymdrech genedlaethol barhaus i gryfhau seiberddiogelwch y DU, codi ymwybyddiaeth y cyhoedd o risgiau seiber, tyfu'r sector seiberddiogelwch, a datblygu ystod eang o alluoedd drwy seiberofod i ymateb i fygythiadau gan weithredwyr gelyniaethus. Er ein bod wedi gwneud cynnydd mawr ac wedi rhoi ein hunain mewn sefyllfa gref, rydym yn dal i wynebu heriau sylweddol ar draws pum colofn y strategaeth hon.

[1] Rydym yn ail ym Mynegai Seiberddiogelwch Byd-eang yr Undeb Telathrebu Rhyngwladol, yn drydydd ym Mynegai Seiberddiogelwch Canolfan Belfer Harvard ac yn ail haen asesiad gallu Seiberddiogelwch y Sefydliad Astudiaethau Strategol Rhyngwladol.

Ecosystem seiber ac arweinyddiaeth dechnolegol y DU

16. Mae dull y DU o adeiladu ei bŵer seiber wedi cynnwys ymdrechion ar y cyd i ddatblygu sylfaen sgiliau seiber y wlad a'i gallu masnachol, gyda llywodraeth y DU a llywodraethau datganoledig Cymru, Gogledd Iwerddon a'r Alban yn gweithio mewn partneriaeth ac yn dysgu oddi wrth ei gilydd. Mae sector seiberddiogelwch y DU yn tyfu'n gyflym, gyda dros 1400 o fusnesau'n cynhyrchu refeniw o £8.9 biliwn y llynedd, yn cynnal 46,700 o swyddi medrus, ac yn denu buddsoddiad sylweddol o dramor. Mae'r sector hwn yn hanfodol i'n pŵer seiber, gan gefnogi ein diogelwch, a'n dylanwad rhyngwladol a'n twf economaidd. Rydym wedi atgyfnerthu enw da'r DU fel arweinydd byd-eang ym maes ymchwil seiberddiogelwch, gyda 19 o ganolfannau rhagoriaeth academaidd a 4 sefydliad ymchwil yn mynd i'r afael â'n heriau seiberddiogelwch mwyaf enbyd.

17. Mae gweithlu'r sector seiberddiogelwch wedi tyfu tua 50% yn ystod y pedair blynedd diwethaf, ac mae'r galw am sgiliau yn aml yn uwch na'r cyflenwad. Rydym wedi ymgysylltu'n helaeth â diwydiant, sefydliadau proffesiynol, myfyrwyr, cyflogwyr, gweithwyr proffesiynol seiberddiogelwch presennol a'r byd academaidd er mwyn deall natur yr her sgiliau seiberddiogelwch yn well. Rydym wedi darparu ystod eang o fentrau allgyrsiol i ysbrydoli pobl ifanc i ddilyn gyrfa ym maes seiberddiogelwch. Rhwng 2019 a 2020, fe wnaethom gynnwys bron i 57,000 o bobl ifanc yn ein rhaglenni dysgu CyberFirst a Cyber Discovery. Fe wnaethom ymestyn ein cyrsiau i gyrraedd myfyrwyr iau ac roedd cystadleuaeth ar-lein CyberFirst i Ferched wedi denu 11,900 o ferched, gyda'r timau gorau yn cystadlu ar yr un pryd mewn 18 lleoliad ar draws y DU. Mae ein rhaglen bwrsari CyberFirst wedi denu israddedigion dawnus a llawn cymhelliant. Y llynedd, roedd 750 o fyfyrwyr yn y cynllun ac roedd y 56 o raddedigion mewn swyddi seiberddiogelwch llawn amser.

18. Er gwaethaf yr ymyriadau hyn, mae'r biblinell sgiliau ehangach yn dal yn her sylweddol: o'r 1.32 miliwn o fusnesau yn yr economi ehangach, mae tua 50% yn dal i ddweud bod ganddynt fwlch sgiliau seiberddiogelwch technegol sylfaenol.[2] Ac er bod sector seiberddiogelwch y DU wedi tyfu'n gyflym, mae'r rhan fwyaf o gwmnïau'n gwmnïau newydd ac mae adeiladu gwerthwyr domestig mawr yn dal yn heriol yn wyneb cyfuno rhyngwladol. Fel y dangosodd y profiad gyda 5G, nid oes gan y DU a'n cynghreiriaid safle blaenllaw mewn rhai rhannau allweddol o'r diwydiant technoleg ehangach. Bydd gwledydd sy'n gallu sefydlu rôl arweiniol yn y technolegau sy'n hanfodol i bŵer seiber mewn sefyllfa well i ddylanwadu ar y ffordd maen nhw'n cael eu dylunio a'u defnyddio, mewn sefyllfa well i ddiogelu eu diogelwch a'u mantais economaidd, ac yn manteisio'n gyflymach ar gyfleoedd i arloesi mewn galluoedd seiber.

Seibergadernid y DU

19. Dros y degawd diwethaf, rydym wedi darparu amrywiaeth eang o ymyriadau gyda'r nod o gryfhau seibergadernid y DU. Mae hyn wedi bod yn bosibl diolch i'r buddsoddiad sylweddol a pharhaus yn rhai o'n galluoedd seiber craidd, gan gynnwys y Ganolfan Seiberddiogelwch Genedlaethol (NCSC), asiantaethau gorfodi'r gyfraith a'n gweithwyr proffesiynol ym maes diogelwch a pholisi ar draws y llywodraeth, yn ogystal â'n partneriaethau domestig a rhyngwladol sy'n ehangu.

[2] Yr Adran dros Dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon, Cyber security skills in the UK labour market 2021 (2021)

20. Ein hymdrechion mwyaf arloesol a blaengar fu gweithredu ar raddfa fawr, gan gynnwys drwy ddatblygu a chynyddu'r gwaith o gyflwyno'r rhaglen Active Cyber Defence (ACD). Y llynedd, fe lwyddodd i drechu 2.3 miliwn ymgyrch faleisus – gan gynnwys 442 ymgyrch gwe-rwydo a oedd yn defnyddio brand y GIG ac 80 o apiau GIG anghyfreithlon a oedd ar gael i'w llwytho i lawr y tu allan i'r siopau apiau swyddogol.[3] Roeddem hefyd wedi cymryd yr awenau yn fyd-eang o ran gwthio bod nwyddau defnyddwyr y gellir cysylltu yn 'ddiogel drwy ddylunio', gan ddatblygu cod ymarfer yn y DU yn 2018 a oedd yn ysbrydoli eraill i ddilyn. Cyfrannodd hyn at safon gyntaf y diwydiant sy'n berthnasol yn fyd-eang ar ddyfeisiau defnyddwyr sydd wedi'u cysylltu â'r rhyngrwyd.[4] [5]

21. Mae rheoliadau newydd wedi cael effaith gadarnhaol ar seiberddiogelwch, gyda 82% o sefydliadau'n dweud bod y gwelliannau roedden nhw wedi'u gwneud wedi cael eu dylanwadu gan gyflwyno Rheoliad Cyffredinol y DU ar Ddiogelu Data yn 2018.[6] Ac mae 77% o fusnesau bellach yn gweld seiberddiogelwch fel blaenoriaeth uchel, cynnydd o 12% ers 2016.[7] Roedd cyflwyno'r Rheoliadau Rhwydweithiau a Systemau Gwybodaeth ('rheoliadau NIS') yn 2018 hefyd wedi arwain at sefydliadau dynodedig yn cymryd camau i sicrhau diogelwch eu rhwydweithiau a'u systemau gwybodaeth yn well, gan arwain at ostyngiad yn y risgiau seiber sy'n gysylltiedig â gwasanaethau hanfodol a gwasanaethau digidol pwysig.[8] Enghraifft dda o gydweithio ar draws pedair gwlad y DU fu'r gwelliannau a wnaed ar draws y sector iechyd, gan gynnwys gweithredu rheoliadau NIS.

22. Rydym wedi darparu cyngor a chanllawiau cynhwysfawr ar seiberddiogelwch i sefydliadau yn yr economi ehangach, a chymorth wedi'i deilwra i sectorau hanfodol yn ystod pandemig y coronafeirws (COVID-19). I'r cyhoedd, mae ein hymgyrch Cyber Aware wedi rhoi cyngor ar y camau y gallant eu cymryd i amddiffyn eu hunain ar-lein. Pan fydd ymosodiadau seiber wedi digwydd, rydym wedi defnyddio ein galluoedd ymateb i ddigwyddiadau sydd gyda'r gorau yn y byd i ddarparu cymorth uniongyrchol yn yr achosion mwyaf difrifol ac mae ein buddsoddiad mewn arbenigwyr gorfodi'r gyfraith lleol yn golygu bod pob digwyddiad sy'n cael ei riportio nawr yn cael ymateb.

23. Rydym wedi sefydlu unedau seiber asiantaethau gorfodi'r gyfraith arbenigol ar draws y DU, ac ochr yn ochr â hyn mae'r rhwydwaith seiber PROTECT, yr Uned Gofal i Ddioddefwyr Troseddau Economaidd a Chanolfannau Seibergadernid rhanbarthol. Mae'r mentrau hyn yn golygu bod rhywun gerllaw neu sy'n hawdd cysylltu â nhw ar gyfer dinasyddion a sefydliadau bach a chanolig a'u bod yn meddu ar y sgiliau a'r wybodaeth leol iawn i ddarparu cymorth ac arweiniad i wella eich seibergadernid.

24. Fodd bynnag, mae gennym fwy a mwy o dystiolaeth o fylchau yn ein cadernid cenedlaethol. Mae lefelau seiberdroseddu a thorri drwy'r diogelwch sy'n effeithio ar lywodraethau, busnesau ac unigolion yn

[3] NCSC, Arolwg Blynyddol NCSC Worldwide 2021(2021)
[4] Yr Adran dros Dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon, Code of Practice for Consumer IoT Security (2018)
[5] Yr Adran dros Dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon, ETSI industry standard based on the Code of Practice (2019)
[6] Yr Adran dros Dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon/RSM, The impact of GDPR on cyber security outcomes (2020); The General Data Protection Regulation (GDPR) that was introduced into UK law in 2018 has now been replaced by the UK GDPR)
[7] Yr Adran dros Dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon, Cyber Security Breaches Survey 2021 (2021)
[8] Yr Adran dros Dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon, Post-Implementation Review of the Network and Information Systems Regulations 2018 (2020)

parhau i godi, yn ogystal â throseddau sydd wedi'u galluogi gan seiber, fel twyll.[9] [10] Mae hen systemau TG, gwendidau yn y gadwyn gyflenwi a phrinder gweithwyr proffesiynol ym maes seiberddiogelwch yn feysydd sy'n peri mwy a mwy o bryder. Mae bron i bedwar busnes o bob deg (39%) a chwarter yr elusennau (26%) yn dweud eu bod wedi dioddef ymosodiadau seiberddiogelwch neu fod eu diogelwch wedi cael ei dorri yn ystod y flwyddyn ddiwethaf, ac mae llawer o sefydliadau (yn enwedig busnesau bach a chanolig) heb y gallu i amddiffyn eu hunain ac ymateb i ddigwyddiadau.[11] Mae diwydiant yn dweud wrthym nad yw llawer o fusnesau'n deall y risgiau seiber maen nhw'n eu hwynebu, nad yw'r cymhellion masnachol i fuddsoddi mewn seiberddiogelwch yn glir, ac nad oes llawer o gymhelliant yn aml i riportio achosion o dorri diogelwch ac ymosodiadau.

Dylanwad ac arweinyddiaeth ryngwladol y DU

25. Yn rhyngwladol, mae ein partneriaid yn parchu arbenigedd seiber y DU ac mae'r DU wedi chwarae rhan allweddol yn y gwaith o gynyddu gallu rhyngwladol a'r gallu i fynd i'r afael â seiber weithgareddau maleisus. Mae hyn wedi cael ei atgyfnerthu gan ddefnyddio ein galluoedd seiber ymosodol mewn ffordd gyfrifol, sy'n cyd-fynd â chyfraith y DU a chyfraith ryngwladol a'n safbwyntiau sydd wedi'u datgan yn gyhoeddus, yn wahanol i weithgareddau annetholus rhai o'n gwrthwynebwyr.

26. Yn ystod ein cyfnod fel Cadeirydd yn Swyddfa'r Gymanwlad, lluniodd ac arweiniodd y DU y gwaith o weithredu Datganiad Seiber y Gymanwlad, ymrwymiad ar y cyd i'n diogelwch, ein ffyniant a'n gwerthoedd mewn seiberofod. Mae rhwydwaith rhyngwladol yr Asiantaeth Troseddu Cenedlaethol (NCA) wedi cryfhau ein partneriaethau gorfodi cyfraith seiber dramor, gan adeiladu ar gysylltiadau sy'n cael eu meithrin drwy hanes hir o ymateb gweithredol cydweithredol. Mae'r DU hefyd wedi tyfu ei rhwydwaith tramor o swyddogion diogelwch seiber a thechnoleg ar draws pum cyfandir ac wedi gwneud gwaith meithrin gallu ar draws 100 o wledydd, gan feithrin cadernid, gwella dylanwad y DU a hyrwyddo gwerthoedd y DU.

27. Mae'r rhaglen Llysgenhadon Seiberddiogelwch wedi datblygu perthnasoedd tymor hir ac wedi helpu busnesau yn y DU i ennill contractau rhyngwladol mawr. Mae ymyriadau datblygu rhyngwladol y DU fel y Rhaglen Mynediad Digidol wedi cydweithio'n llwyddiannus â gwledydd partner yn Affrica, Asia ac America Ladin drwy ddarparu cyngor technegol i wella capasiti seiberddiogelwch eu llywodraeth, eu sectorau busnes a'u defnyddwyr – gan gynnwys drwy gynyddu sgiliau hylendid seiber mewn cymunedau sy'n cael eu gwasanaethu'n wael er mwyn i'r bobl fwyaf agored i niwed allu amddiffyn eu hunain rhag risgiau a heriau bod ar-lein.

28. Fodd bynnag, rydym yn wynebu dulliau sy'n cystadlu â'i gilydd yn rhyngwladol wrth i gystadleuwyr systemig fel Tsieina a Rwsia barhau i ddadlau dros fwy o sofraniaeth genedlaethol dros seiberofod fel ateb i heriau diogelwch. Mae rhyddid y rhyngrwyd yn lleihau'n fyd-eang ac mae'r weledigaeth o'r rhyngrwyd fel gofod a rennir sy'n cefnogi cyfnewid gwybodaeth a nwyddau rhwng cymdeithasau agored yn dod o dan fygythiad.

---

[9] A ddiffinnir fel troseddau Deddf Camddefnyddio Cyfrifiaduron

[10] Y Swyddfa Ystadegau Gwladol, Troseddau yng Nghymru a Lloegr: y flwyddyn sy'n gorffen ym Mehefin 2021 (2021)

[11] Yr Adran dros Dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon, Cyber Security Breaches Survey 2021 (2021)

Mynd i'r afael â bygythiadau seiber i'r DU a rhwystro ein gwrthwynebwyr

29. Mae'r bygythiadau rydym yn eu hwynebu mewn seiberofod a thrwyddo wedi cynyddu o ran dwysedd, cymhlethdod a difrifoldeb yn ystod y blynyddoedd diwethaf. Mae ymosodiadau seiber yn erbyn y DU yn cael eu cynnal gan ystod gynyddol o weithredwyr gwladwriaethol, grwpiau troseddol (weithiau'n gweithredu yn ôl cyfarwyddyd gwladwriaethau neu gyda'u cymeradwyaeth ymhlyg) ac ymgyrchwyr at ddibenion ysbïo, enillion masnachol, difrod a thwyllwybodaeth. Mae ymosodiadau o'r fath yn achosi colled ariannol sylweddol, dwyn eiddo deallusol, trallod seicolegol, tarfu ar wasanaethau ac asedau a risgiau i'n seilwaith cenedlaethol hanfodol, sefydliadau democrataidd a'r cyfryngau. Maent hefyd yn gallu niweidio hyder buddsoddwyr a defnyddwyr a chynyddu'r anghydraddoldebau a'r niwed sydd eisoes yn bodoli. Yn ystod pandemig COVID-19, cafodd y pandemig cysgodol o drais ar sail rhywedd ei waethygu gan ymosodiadau ar-lein. Mae ymosodiadau meddalwedd wystlo yn dal i ddod yn fwy soffistigedig a niweidiol. Er bod lefel gyffredinol y bygythiad seiber oddi wrth weithredwyr gelyniaethus yn ystod pandemig COVID-19 wedi aros yn gyson, maent wedi manteisio arno fel cyfle ac wedi symud eu gweithrediadau seiber i ddwyn ymchwil ar frechlynnau ac ymchwil feddygol, ac i danseilio gwledydd eraill sydd eisoes wedi'u llesteirio gan yr argyfwng. Mae'r ddibyniaeth gynyddol ar dechnolegau digidol ar gyfer gweithio o bell a thrafodion ar-lein hefyd wedi cynyddu'r cysylltiad â risgiau. Ochr yn ochr â hyn, mae'r rhaniadau digidol hefyd wedi creu mynediad anwastad at wasanaethau ar-lein ac wedi datgelu pobl i gam-drin a niwed ar-lein oherwydd diffyg llythrennedd digidol ac ymwybyddiaeth o'r mesurau seiberddiogelwch y gallwn ni i gyd eu cymryd i fod yn ddiogel ar-lein.[12]

30. Mae'r Llywodraeth wedi cymryd camau i wrthsefyll y bygythiadau cynyddol hyn. Mae buddsoddiad sylweddol yn ein galluoedd cudd-wybodaeth wedi gwella ein dealltwriaeth o'r bygythiad ac wedi golygu ein bod yn gallu cynnal gwrth-ymgyrchoedd cudd mwy effeithiol. Rydym wedi datblygu ymateb integredig o ran gorfodi'r gyfraith gyda seiberdroseddau, dan arweiniad yr Asiantaeth Troseddu Cenedlaethol (NCA) a thimau seiber pwrpasol o fewn unedau troseddu cyfundrefnol rhanbarthol a heddluoedd lleol ledled Cymru, Lloegr, Gogledd Iwerddon a'r Alban. Mae hyn wedi gwella ein dylanwad gweithredol ac ymchwiliol dros seiberdroseddwyr a gwrthwynebwyr eraill. Mae'r llywodraeth hefyd yn cryfhau diogelwch y nifer cynyddol o ddatrysiadau hunaniaeth ddigidol, drwy ddatblygu fframwaith ymddiriedaeth hunaniaeth a phriodweddau digidol y DU.[13] Bydd hyn hefyd yn helpu i fynd i'r afael â throseddau sy'n ymwneud â chamddefnyddio data hunaniaeth. Ac mae rhaglen Cyber Choices yr NCA yn helpu pobl i wneud dewisiadau mwy gwybodus, gan eu troi oddi wrth droseddu i ddefnyddio eu sgiliau seiber mewn ffordd gadarnhaol a chyfreithiol.

31. Rydym wedi buddsoddi'n sylweddol yn ein galluoedd seiber ymosodol, yn gyntaf drwy'r Rhaglen Seiber Ymosodol Genedlaethol, ac yn fwy diweddar drwy sefydlu'r Llu Seiber Cenedlaethol (NCF). Mae'r NCF yn dwyn ynghyd staff o Bencadlys Cyfathrebu Llywodraeth y DU (GCHQ), y Weinyddiaeth Amddiffyn (MOD), y Gwasanaeth Cudd-wybodaeth Cyfrinachol (SIS, a elwir hefyd yn MI6) a'r Labordy Technoleg a Gwyddoniaeth Amddiffyn, dan un gorchymyn unedig am y tro cyntaf. Mae'n gweithredu mewn seiberofod a thrwyddo i gadw'r wlad yn ddiogel ac i ddiogelu ac i hyrwyddo buddiannau'r DU gartref a thramor.

[12] NCSC, CyberAware

[13] Yr Adran dros Dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon, UK digital identity and attributes trust framework (2021)

32. Ochr yn ochr â'n cynghreiriaid, rydym hefyd wedi ceisio cynyddu cost gweithgarwch gelyniaethus a noddir gan wladwriaethau mewn seiberofod drwy briodoli ymosodiadau – fel y gwnaethom pan dorrwyd diogelwch SolarWinds a Microsoft Exchange yn ddiweddar – a rhoi canlyniadau i'r rheini sy'n gyfrifol. Mae datblygu trefn sancsiynau seiber ymreolaethol y DU wedi ychwanegu adnodd tarfu arall rydym wedi'i ddefnyddio i ymateb i ddigwyddiadau fel ymosodiadau WannaCry a NotPetya. Fodd bynnag, er gwaethaf hyn i gyd, yn y bôn nid yw'n ymddangos bod ein dull o ataliaeth seiber wedi newid y calcwlws risg ar gyfer ymosodwyr eto. Caiff rhai enghreifftiau diweddar o ymosodiadau seiber sylweddol eu disgrifio isod.

Astudiaethau achos diweddar o ymosodiadau seiber

Yn ystod 2021, aeth y DU ati i weithio gyda phartneriaid byd-eang i ganfod ac amharu ar fygythiadau a rennir, roedd y rhai mwyaf cyson o'r rhain yn deillio o Rwsia a Tsieina. Yn ogystal â'r bygythiadau seiberddiogelwch uniongyrchol a achosir gan y wladwriaeth yn Rwsia, daeth yn amlwg bod llawer o'r gangiau troseddu cyfundrefnol a oedd yn lansio ymosodiadau meddalwedd wystlo yn erbyn targedau'r Gorllewin wedi'u lleoli yn Rwsia. Roedd Tsieina yn dal yn weithredwr soffistigedig iawn mewn seiberofod gyda mwy a mwy o uchelgais i gyfleu ei dylanwad y tu hwnt i'w ffiniau a diddordeb amlwg yng nghyfrinachau masnachol y DU. Mae'n debyg mai sut bydd Tsieina'n esblygu yn y degawd nesaf fydd y prif sbardun ar gyfer seiberddiogelwch y DU yn y dyfodol. Er nad oeddent mor soffistigedig â Rwsia a Tsieina, roedd Iran a Gogledd Korea wedi parhau i ddefnyddio ymyriadau digidol i gyflawni eu hamcanion, gan gynnwys drwy ddwyn a difrodi.

Seiberdroseddwyr yn defnyddio meddalwedd wystlo i ymosod ar wasanaethau cyhoeddus

Meddalwedd wystlo oedd y bygythiad seiber mwyaf i'r DU yn 2021. Oherwydd effaith debygol ymosodiad llwyddiannus ar wasanaethau hanfodol neu seilwaith cenedlaethol hanfodol, mae'r NCSC wedi asesu bod meddalwedd wystlo yr un mor niweidiol ag ysbïo a noddir gan wladwriaeth.[14]

Ym mis Hydref 2020, dioddefodd Cyngor Hackney ymosodiad seiber meddalwedd wystlo a achosodd fisoedd lawer o aflonyddwch ac a gostiodd filiynau o bunnoedd i'w gywiro. A hithau'n adeg dyngedfennol wrth ddelio ag effaith pandemig COVID-19, cafodd y cyngor ei gloi allan o ddata pwysig ac amharwyd ar lawer o wasanaethau, gan gynnwys y dreth gyngor a thaliadau budd-daliadau. Mae awdurdodau lleol eraill wedi dioddef ymosodiadau tebyg, fel y mae amryw o sefydliadau yn y sector addysg.

[14] NCSC, Mitigating malware and ransomware attacks (2021)

Ym mis Mai 2021, fe wnaeth ymosodiad meddalwedd wystlo yn erbyn Awdurdod Gweithredol Iechyd Iwerddon darfu ar ysbytai a rhwydweithiau TG gofal iechyd Iwerddon am dros 10 diwrnod, gan achosi canlyniadau go iawn i gleifion a'u teuluoedd. Cafodd rhywfaint o'r data cleifion a gafodd ei ddwyn ei gyhoeddi ar-lein hefyd. Roedd yr Awdurdod Gweithredol Iechyd, sy'n darparu gwasanaethau iechyd a gofal cymdeithasol yn Iwerddon, wedi cau rhwydweithiau cenedlaethol a rhanbarthol yr un diwrnod i gyfyngu ar y digwyddiad. Cafwyd gweithgareddau seiber maleisus ar rwydwaith Adran Iechyd Iwerddon hefyd, ond oherwydd y defnyddiwyd offer yn ystod y broses ymchwilio cafod ymgais i ddefnyddio meddalwedd wystlo ei chanfod a'i stopio. Roedd yr ymosodiad hefyd wedi effeithio ar Ogledd Iwerddon, gan effeithio ar y gallu i gael gafael ar ddata a oedd gan yr Awdurdod Gweithredol Iechyd ar gyfer rhai gwasanaethau trawsffiniol i gleifion.

Yn bwysig iawn, ni chafodd taliad ei wneud yn y naill achos na'r llall. **Nid yw asiantaethau gorfodi'r gyfraith yn hybu, yn ardystio nac yn cymeradwyo talu arian yn dilyn yr ymosodiadau hyn. Os ydych chi'n talu:**

- **nid oes sicrwydd y cewch chi fynediad at eich data neu eich cyfrifiadur**
- **bydd eich cyfrifiadur yn dal i fod wedi'i heintio**
- **byddwch yn talu grwpiau troseddol**
- **rydych chi'n fwy tebygol o gael eich targedu yn y dyfodol**

Mae'r NCSC yn cyhoeddi canllawiau ar sut mae amddiffyn sefydliadau rhag ymosodiadau maleiswedd neu feddalwedd wystlo, gan gynnwys sut mae paratoi ar gyfer digwyddiad a chamau i'w cymryd os yw eich sefydliad eisoes wedi'i heintio.

Gwladwriaethau sy'n ecsbloetio cadwyni cyflenwi a gwendidau strategol

Roedd yr hyn a ddigwyddodd i'r cwmni meddalwedd SolarWinds ac ecsbloetio Gweinyddion Microsoft Exchange yn tynnu sylw at y bygythiad o ymosodiadau ar y gadwyn gyflenwi. Roedd yr ymosodiadau soffistigedig hyn, lle'r oedd gweithredwyr yn targedu elfennau llai diogel – fel darparwyr gwasanaethau a reolir neu blatfformau meddalwedd masnachol – yng nghadwyn gyflenwi sefydliadau economaidd, llywodraethol a diogelwch cenedlaethol yn ddau o'r ymyriadau seiber mwyaf difrifol a welwyd erioed gan yr NCSC.

Ddechrau mis Rhagfyr 2020, canfu cwmni seiberddiogelwch o UDA, FireEye, fod ymosodwr wedi gallu ychwanegu addasiad maleisus at gynnyrch y mae ef a llawer o sefydliadau eraill ledled y byd yn ei ddefnyddio. Roedd yr addasiad hwn yn caniatáu i'r ymosodwr anfon gorchmynion lefel gweinyddwr i unrhyw fersiwn o'r cynnyrch hwnnw a oedd wedi'i osod ac yr effeithiwyd arno a gellid ei ddefnyddio ar gyfer ymosodiadau pellach wedi'u targedu ar systemau cysylltiedig. Cafodd yr ymosodiad cadwyn gyflenwi cychwynnol ei wneud drwy ddarn o feddalwedd o'r enw Orion, ac offer monitro rhwydwaith TG a ddatblygwyd gan gwmni o'r enw **SolarWinds**. Roedd y gweithredwr yn gallu rhoi cod maleisus mewn ffeil diweddariad ar gyfer y meddalwedd, cyn belled yn ôl â mis Mawrth 2020. Ym mis Ebrill 2021, datgelodd yr NCSC am y tro cyntaf, ynghyd â'i gymheiriaid diogelwch yn yr Unol Daleithiau, mai Gwasanaeth Cudd-wybodaeth Tramor Rwsia (yr SVR) oedd y tu ôl i'r ymosodiad hwn – un o'r ymosodiadau seiber mwyaf difrifol yn ddiweddar.[15] Cadarnhaodd SolarWinds fod hyn wedi effeithio ar 18,000 o sefydliadau ar draws y byd, gan gynnwys adrannau Llywodraeth yr Unol Daleithiau. Roedd y digwyddiad hwn

[15] FCDO, Russia: UK and US expose global campaign of malign activity by Russian intelligence services (2021)

yn rhan o batrwm ehangach o ymyriadau seiber gan yr SVR sydd wedi ceisio cael mynediad at rwydweithiau TG aelodau a llywodraethau NATO ar draws Ewrop yn y gorffennol.

Ar 2 Mawrth 2021, datgelodd Microsoft fod gweithredwyr soffistigedig wedi ymosod ar nifer o weinyddion **Microsoft Exchange**, sy'n cael eu defnyddio gan sefydliadau ar draws y byd i reoli eu e-bost, eu hamserlenni a'u cydweithio. Roedd Microsoft wedi asesu bod yr ymyriadau cychwynnol wedi dechrau mor gynnar â mis Ionawr 2021 a'u bod wedi'u noddi gan wladwriaeth Tsieina. Mewn ymateb i hyn, fe wnaethant ryddhau mwy nag un diweddariad diogelwch ar gyfer y gweinyddion yr effeithiwyd arnynt. Ym mis Gorffennaf 2021, ymunodd y DU â phartneriaid o'r un anian i gadarnhau mai gweithredwyr a oedd yn cael cefnogaeth gan wladwriaeth Tsieina oedd yn gyfrifol am yr ymosodiadau a effeithiodd ar dros chwarter miliwn o weinyddion ledled y byd.[16] Roedd yr ymosodiad yn debygol iawn o alluogi ysbïo ar raddfa fawr, gan gynnwys cael gwybodaeth bersonol adnabyddadwy ac eiddo deallusol. Roedd peryglu Microsoft Exchange wedi golygu bod y drwgweithredwr wedi cael ei droed i mewn i fynd ymhellach i rwydweithiau TG dioddefwyr. Adeg yr ymosodiad, roedd y llywodraeth wedi rhoi cyngor yn gyflym ac wedi argymell camau gweithredu i'r rheini yr oedd hyn yn effeithio arnynt, a dywedodd Microsoft fod 92% o gwsmeriaid wedi gosod diweddariad yn erbyn y gwendid erbyn diwedd mis Mawrth.

[16] FCDO, UK and allies hold Chinese state responsible for a pervasive pattern of hacking (2021)

Sbardunwyr newid

33. Yn ystod y degawd nesaf, **bydd data a chysylltedd digidol yn parhau i dyfu'n gyflym i bron pob agwedd ar ein bywydau**. Mae twf byd-eang enfawr mewn defnydd a mynediad i'r Rhyngrwyd, wedi'i ategu gan ddata a'r seilwaith y mae'r defnydd o ddata'n dibynnu arno, yn creu marchnadoedd newydd ac yn cynyddu hwylustod, dewis ac effeithlonrwydd. Ond mae hefyd yn gwneud gwledydd yn llawer mwy dibynnol ar systemau digidol cysylltiedig, gan ddarparu mwy o gyfleoedd ar gyfer gweithgarwch maleisus ac effaith sylweddol ar y 'byd go iawn'. Wrth i dechnolegau critigol a heb fod yn rhai critigol barhau i gydgyfarfod ar draws sectorau, mae'r risgiau hyn yn ymledu i feysydd newydd yn ein heconomi, ac mae symud data a gwasanaethau i'r cwmwl – ac yn aml y tu allan i'r DU – yn ein gwneud yn fwy agored byth i niwed.

34. Rydym yn gweld mwy a mwy o ryngweithio rhwng busnesau sydd wedi ennill eu plwyf mewn sectorau sy'n cael eu rheoleiddio, fel telathrebu ac ynni, a busnesau newydd nad ydynt yn cael eu rheoleiddio i raddau helaeth, fel y rheini sy'n darparu dulliau microgynhyrchu, gwefru cerbydau trydan neu 'fannau cysylltiedig'. Bydd seilweithiau critigol yn llawer mwy gwasgaredig ac ar led ac mae hyn yn newid yn sylfaenol sut bydd rheoleiddio'n effeithio ar ddiogelwch y swyddogaethau a'r gwasanaethau hanfodol rydym yn dibynnu arnynt. Bydd yr arallgyfeirio hwn hefyd yn effeithio ar ein diogelwch gwladol ehangach, gan ei gwneud yn anoddach cael gafael ar wybodaeth, boed hynny ar gyfer gorfodi'r gyfraith neu seiberddiogelwch. Bydd y newid hwn yn yr amgylchedd hefyd yn effeithio ar gynnyrch a gwasanaethau yn ehangach y tu allan i'n seilwaith cenedlaethol hanfodol traddodiadol.

35. Bydd y **dirwedd gynyddol gymhleth** hon yn ei gwneud yn anoddach fyth i wladwriaethau, busnesau a chymdeithas ddeall y risgiau y maent yn eu hwynebu a sut y dylent ddiogelu eu hunain a sut y gallant wneud hynny. Mae mwy o ddibyniaeth ar gyflenwyr trydydd parti i ddarparu gwasanaethau a reolir, sydd yn aml â mynediad breintiedig at systemau TG miloedd o gleientiaid, yn creu risgiau newydd y mae angen rhoi sylw iddynt. Bydd dyfeisiau a rhwydweithiau'n cael eu cysylltu fwyfwy â'r rhyngrwyd fel mater o drefn, gan ymestyn seiberofod i'n cartrefi, ein cerbydau, ein hamgylchedd adeiledig a'n seilwaith diwydiannol. Bydd synwyryddion, dyfeisiau mae modd eu gwisgo, dyfeisiau meddygol a biometreg yn cymylu'r ffin ymhellach rhwng gweithgarwch all-lein ac ar-lein. Bydd risgiau seiber yn treiddio, gan gynyddu faint o ddata personol a sensitif sy'n cael ei gynhyrchu a'r effaith bosibl os bydd diogelwch systemau'n cael ei dorri.

36. Yn y cyd-destun hwn, bydd y **bygythiadau mewn seiberofod yn parhau i esblygu ac arallgyfeirio** wrth i alluoedd seiber o'r radd flaenaf gael eu hyrwyddo a'u lledaenu i ystod ehangach o wladwriaethau a grwpiau troseddol. Bydd nifer y gweithredwyr sydd â'r gallu a'r bwriad i dargedu'r DU mewn seiberofod yn cynyddu a bydd gwladwriaethau'n defnyddio ystod ehangach o ysgogiadau i gynnal gweithgareddau aflonyddol, gan gynnwys defnyddio gweithredwyr procsi. Mae'r newid cyflym i weithio hybrid a'r cyfyngiadau ar deithio rhyngwladol sy'n deillio o'r pandemig wedi arwain at fwy o ddibyniaeth ar wasanaethau digidol ac wedi cymell grwpiau troseddau cyfundrefnol i gyflawni seiberdroseddau. Rydym eisoes yn dechrau gweld arwyddion o'r duedd hon, gyda'r arolwg troseddau diweddaraf yn amcangyfrif bod seiberdroseddau wedi cynyddu'n sylweddol rhwng 2019 a 2021.[17]

[17] Y Swyddfa Ystadegau Gwladol, Troseddau yng Nghymru a Lloegr: y flwyddyn yn gorffen Mehefin 2021 (2021)

Ni fydd yr her hon yn unigryw i'r DU, mae pawb sy'n dibynnu ar seiberofod yr un mor agored i niwed.

37. Bydd mwy o gystadleuaeth mewn seiberofod wrth i weithredwyr gwladwriaethol ac anwladwriaethol geisio cael mantais strategol mewn seiberofod a thrwyddo. Bydd gweithrediadau seiber yn dod yn bwysicach o ran cyfleu pŵer o dan drothwy gwrthdaro arfog ac mewn sefyllfaoedd cyn gwrthdaro. Bydd gwrthdaro yn y dyfodol hefyd yn arwain at gynnydd yn y defnydd o alluoedd seiber. Er mwyn i'r DU weithredu'n effeithiol, bydd angen lefelau uwch o seibergadernid arnom yn ein galluoedd amddiffyn. Bydd angen integreiddio gweithrediadau seiber ag elfennau grym eraill er mwyn trechu bygythiadau a galluogi gweithgarwch amddiffyn ehangach. Bydd y gofod yn dod yn faes lle ceir mwy o weithgarwch, fel y nodir yn y Strategaeth Gofod Genedlaethol, gan agor meysydd risg newydd ar yr un pryd â chreu cyfleoedd i'r DU fanteisio ar ei gallu seiber i sicrhau mantais mewn ffyrdd newydd.[18]

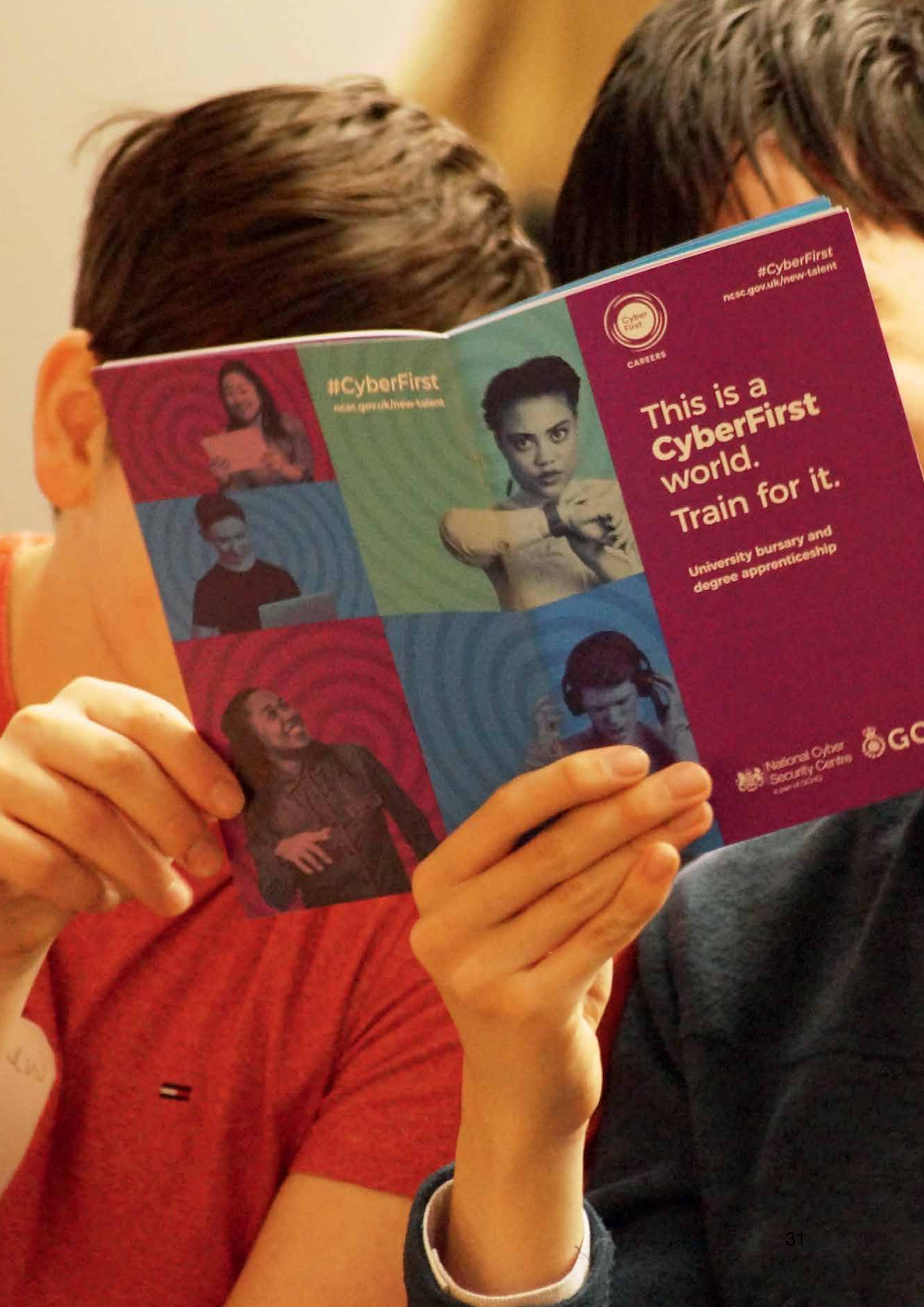
38. Bydd dadleuon ynghylch y rheolau sy'n rheoli seiberofod yn dod yn faes o **gystadleuaeth systemig rhwng pwerau mawr,** gyda gwerthoedd yn gwrthdaro rhwng gwledydd sydd am gadw system sy'n seiliedig ar gymdeithasau agored a chystadleuwyr systemig fel Tsieina a Rwsia sy'n hyrwyddo mwy o reolaeth gan y wladwriaeth fel yr unig ffordd o ddiogelu seiberofod. Bydd hyn yn rhoi pwysau ar y rhyngrwyd agored ac am ddim, wrth i wladwriaethau, cwmnïau technoleg mawr a gweithredwyr eraill hyrwyddo dulliau sy'n cystadlu â'i gilydd o ran safonau technegol a llywodraethu'r rhyngrwyd.

39. Bydd hyn yn cael ei waethygu gan **gystadleuaeth am reolaeth ar dirwedd dechnolegol sy'n esblygu'n gyflym**. Wrth i dechnoleg ddigidol gael ei hintegreiddio i'n bywydau bob dydd, busnesau a seilwaith, mae rhai technolegau'n dod yn wirioneddol hanfodol i weithrediad cymdeithas. Bydd mwy a mwy o bŵer yn cael ei ddal gan wledydd sydd â mantais strategol mewn gwyddoniaeth a thechnoleg a mynediad at y data sy'n ysgogi arloesedd, gan eu galluogi i ddylanwadu ar eraill a siapio safonau byd-eang mewn ffyrdd sy'n gweddu orau i'w buddiannau economaidd a gwleidyddol eu hunain.

40. Bydd **technolegau newydd** fel gefeilliaid digidol, cyfrifiadura cwantwm, a systemau awtonomaidd ar raddfa fawr – a'r wybodaeth maent yn ei chynhyrchu – yn creu cyfleoedd a risgiau newydd ac yn agor galluoedd seiber newydd ar gyfer ymosodwyr ac amddiffynwyr, yn yr un modd ag y mae cryptoarian yn cael ei ddefnyddio gan gangiau meddalwedd wystlo. Mae arweinyddiaeth ym maes technoleg ar fwy o wasgar, ac ni fydd y DU yn gallu datblygu gallu sofran yn yr holl dechnolegau sy'n bwysig. Mae gwladwriaethau a chwmnïau yn defnyddio safonau technegol i hyrwyddo eu buddiannau eu hunain ac mae perygl i dechnolegau allweddol gael eu siapio gan y rheini nad ydynt yn rhannu ein gwerthoedd.

41. Ers dros ddegawd, mae'r DU wedi mynd ar drywydd strategaeth seiberddiogelwch genedlaethol uchelgeisiol ac wedi cynnal lefel sylweddol o fuddsoddiad, gan sefydlu'r wlad fel arweinydd byd-eang ym maes seiber. Fel sy'n amlwg o'r dadansoddiad uchod, mae heriau a chyfleoedd sylweddol yn dal i fodoli. Mae'r adrannau canlynol yn amlinellu ein hymateb cenedlaethol.

[18] Llywodraeth Ei Mawrhydi, National Space Strategy (2021)


#CyberFirst
ncsc.gov.uk/new-talent
CAREERS
This is a CyberFirst world. Train for it.
University bursary and degree apprenticeship
National Cyber Security Centre

Ein Hymateb Cenedlaethol

42. Yn yr amgylchedd strategol hwn, mae gan y DU ddewis i'w wneud. Fe allen ni geisio mynd bob yn gam â'r bygythiadau a'r heriau rydyn ni'n eu hwynebu mewn seiberofod sy'n fwyfwy cymhleth, gan gyfuno cynnydd y pum mlynedd diwethaf a mynd i'r afael â'r materion mwyaf brys lle gallwn ni. Mae dwy risg i'r dull hwn. Y cyntaf yw nad ydym yn llawn sylweddoli potensial cryfder y DU ym maes seiber i gefnogi blaenoriaethau cenedlaethol, a'n bod yn colli cyfleoedd. Yr ail risg fwy difrifol yw ein bod yn cyrraedd trobwynt technolegol, ac yn gweld bod sylfeini ein heconomi a'n cymdeithas yn y dyfodol yn cael eu siapio gan ein cystadleuwyr a'n gwrthwynebwyr, ac y bydd yn rhaid inni weithio'n galetach i sicrhau ein diogelwch ein hunain.

43. Ein barn ni yw, wrth i seiberofod ddod yn bwysicach fyth i'n buddiannau ni ac i fuddiannau ein cynghreiriaid a'n gwrthwynebwyr, **mae'n rheidrwydd strategol i feithrin ein mantais gystadleuol wrth fynd i'r afael â'r dirwedd hon**. Bydd hyn yn ein galluogi nid yn unig i sicrhau ein diogelwch heddiw ond hefyd i siapio a manteisio ar fyd yfory.

Ein gweledigaeth, ein nodau a'n hegwyddorion

44. Ein gweledigaeth yw y bydd y **DU yn 2030 yn parhau i fod yn bŵer seiber cyfrifol a democrataidd blaenllaw, a fydd yn gallu diogelu a hyrwyddo ein buddiannau mewn seiberofod a thrwyddo i gefnogi nodau cenedlaethol**.

45. Er mwyn gwireddu'r weledigaeth hon, byddwn yn mynd ar drywydd pum nod strategol. Nod pob un yw cryfhau ein cryfder cenedlaethol yn un o bum dimensiwn pŵer seiber, a chyda'i gilydd, eu nod yw gwella ein gallu i gynnal seiberofod sy'n adlewyrchu ein gwerthoedd a'n buddiannau. Mae'r pum nod hyn – neu golofn – yn fframwaith strategol i lywio ein gweithgarwch, ac mae Rhan 2 yn nodi'r camau y byddwn yn eu cymryd hyd at 2025 o dan bob un.

- **Colofn 1: Cryfhau ecosystem seiber y DU**, buddsoddi yn ein pobl a'n sgiliau a dyfnhau'r bartneriaeth rhwng llywodraeth, y byd academaidd a diwydiant
- **Colofn 2: Adeiladu DU ddigidol gydnerth a ffyniannus**, lleihau risgiau seiber er mwyn i fusnesau allu cynyddu manteision economaidd technoleg ddigidol a bod dinasyddion yn ddiogel ar-lein ac yn hyderus bod eu data'n cael ei ddiogelu
- **Colofn 3: Cymryd yr awenau gyda'r technolegau sy'n hanfodol i bŵer seiber,** adeiladu ein gallu diwydiannol a datblygu fframweithiau i ddiogelu technolegau'r dyfodol
- **Colofn 4: Hyrwyddo arweinyddiaeth a dylanwad byd-eang yn y DU ar gyfer trefn ryngwladol sy'n fwy diogel, ffyniannus ac agored**, gan weithio gyda phartneriaid mewn llywodraeth a diwydiant a rhannu arbenigedd sy'n sail i bŵer seiber y DU
- **Colofn 5: Canfod, atal ac amharu ar ein gwrthwynebwyr er mwyn gwella diogelwch y DU mewn seiberofod a thrwyddo**, defnyddio sbectrwm llawn ysgogiadau'r DU mewn ffordd sy'n fwy integredig, creadigol a rheolaidd

46. Bwriedir i'r nodau hyn atgyfnerthu ei gilydd. Er enghraifft, bydd cyflawni lefelau uwch o seiberddiogelwch a seibergadernid yn ddomestig yn sylfaen angenrheidiol ar gyfer safiad mwy gweithredol yn rhyngwladol. Yn ei dro, mae ein cadwyni cyflenwi byd-eang a'r bygythiadau rydym yn eu hwynebu o dramor yn golygu na fyddwn yn gallu sicrhau ein diogelwch ein hunain heb siapio ymddygiad gweithredwyr rhyngwladol yn fwy gweithredol. A bydd ein gallu i ddylanwadu ar ddadleuon byd-eang ar seiberofod, y rhyngrwyd a thechnoleg yn dibynnu ar gynnal ein mantais dechnegol ac adeiladu ecosystem arloesi sy'n creu mantais wirioneddol yn y technolegau sydd bwysicaf.

47. Yn ganolog i'n gweledigaeth mae **hyrwyddo seiberofod agored, heddychlon a diogel sy'n rhad ac am ddim**. Nid yw ein ffocws strategol ar bŵer seiber yn golygu procio gwrthdaro na pharatoi'r DU i ennill gêm sero-swm. Fel y mae'r Adolygiad Integredig yn ei nodi, byd lle gall cymdeithasau agored ac economïau ffynnu yw'r warant orau ar gyfer ein ffyniant, ein sofraniaeth a'n sicrwydd yn y dyfodol. Bydd y DU yn gweithio gyda gwledydd o'r un anian i hyrwyddo ein gwerthoedd cyffredin o fod yn agored ac yn ddemocrataidd, gan ddilyn **ymagwedd gyfrifol a democrataidd at bŵer seiber**. Mae hyn yn golygu, wrth weithio at y pum nod strategol hyn, y byddwn yn dilyn yr egwyddorion **canlynol**:

- Byddwn yn blaenoriaethu gallu dinasyddion a busnesau i weithredu mewn seiberofod yn ddiogel er mwyn iddynt allu manteisio i'r eithaf ar fanteision economaidd a chymdeithasol technoleg ddigidol ac arfer eu hawliau cyfreithiol a democrataidd

- Byddwn yn gweithio i gynnal rhyngrwyd agored a rhyngweithredol fel y model gorau i gefnogi ffyniant a lles byd-eang, gan wrthsefyll pwysau gwladwriaethau awdurdodaidd at ddarnio a'u syniad o sofraniaeth rhyngrwyd

- Byddwn yn gwneud defnydd cyfreithlon, cymesur a chyfrifol o'n galluoedd seiber, wedi'i ategu gan oruchwyliaeth ac ymgysylltiad clir â'r cyhoedd a'n cynghreiriaid, a byddwn yn dal eraill i gyfrif am ymddygiad di-hid neu annetholus mewn seiberofod

- Byddwn yn gwneud popeth gallwn ni i rwystro defnyddio seiberofod mewn ffordd droseddol. Byddwn yn mynd ar drywydd y rheini sy'n defnyddio procsi troseddol neu sy'n cuddio grwpiau troseddol yn eu tiriogaethau. Byddwn yn gweithio i atal y cynnydd mewn galluoedd seiber o'r radd flaenaf ymysg troseddwyr

- Byddwn yn hyrwyddo dull cynhwysol sy'n cynnwys nifer o randdeiliaid mewn trafodaethau am ddyfodol seiberofod a thechnoleg ddigidol, gan gynnal hawliau dynol mewn seiberofod a mynd i'r afael â symudiadau at awdurdodyddiaeth ddigidol a rheolaeth y wladwriaeth

Newidiadau allweddol yn ein dull gweithredu

48. Mewn sawl maes, bydd ein strategaeth yn adeiladu ar ein dull gweithredu presennol, gan geisio gwella, ehangu neu addasu ein hymdrechion lle bo angen. Mae'r prif wahaniaethau o Strategaeth Seiberddiogelwch Genedlaethol 2016-2021 wedi'u nodi isod ac maent yn adlewyrchu ein huchelgais ehangach i gryfhau safle'r DU fel un o'r prif bwerau seiber.

49. Ymrwymiad i sicrhau bod y DU ar flaen y gad o ran seiber. Bydd y llywodraeth yn buddsoddi £2.6 biliwn mewn seiber a hen TG dros y tair blynedd nesaf. Mae hyn yn ychwanegol at fuddsoddiad sylweddol yn y Llu Seiber Cenedlaethol a gyhoeddwyd yn yr Adolygiad o Wariant 2020 (SR20). Mae'n cynnwys cynnydd o £114 miliwn yn y Rhaglen Seiberddiogelwch Genedlaethol; ac mae hyn ochr yn ochr â chynnydd mewn buddsoddiad a gyhoeddwyd hefyd mewn ymchwil a datblygu, cudd-wybodaeth, amddiffyn, arloesi, seilwaith a sgiliau, a bydd pob un ohonynt yn cyfrannu'n rhannol at bŵer seiber y DU. Mae buddsoddiad mewn seiber a gyhoeddwyd yn Adrolygiad o Wariant 2020 ac Adolygiad o Wariant 2021 (SR21) yn llawer mwy na'r £1.9 biliwn dros bum mlynedd a ymrwymwyd i'r strategaeth flaenorol.[19]

50. Strategaeth Seiber Genedlaethol fwy cynhwysfawr. Mae seiberddiogelwch yn dal wrth galon y strategaeth hon, ond mae nawr yn dod ag ystod lawn galluoedd y DU at ei gilydd y tu mewn a'r tu allan i lywodraeth. Mae'n rhoi mwy o bwyslais ar y seilwaith a'r technolegau hanfodol sy'n sail i seiberofod, yn helpu cwmnïau seiber yn y DU i dyfu'n ddomestig ac i gystadlu'n rhyngwladol, yn cymryd camau gweithredu rhyngwladol i siapio a dylanwadu ar ddyfodol seiberofod, ac yn integreiddio seiber ymosodol fel ysgogwr pŵer. Mae'n galw am ddull gweithredu strategol cenedlaethol cwbl gydlynol. Mae'r strategaeth yn dosbarthu cyfrifoldebau am arweinyddiaeth a chydlynu ar draws yr Ysgrifenyddion Gwladol, ac mae'n ymwneud yn llawer agosach â'r gweinyddiaethau datganoledig. Mae hyn yn adeiladu ar ein llwyddiant o ran cydlynu ymdrechion ar draws y llywodraeth, sy'n un o gryfderau allweddol y DU.

[19] Trysorlys Ei Mawrhydi, Autumn Budget and Spending Review 2021 (2021)

51. Ymdrech cymdeithas gyfan. Ein nod yw cael dull gweithredu strategol cenedlaethol sy'n cael ei siapio gan ac sy'n helpu i lywio'r broses o wneud penderfyniadau mewn sefydliadau ar hyd a lled y wlad; ac sy'n darparu'r sylfaen ar gyfer cydweithio cryfach gyda'n partneriaid yn y DU ac ar draws y byd. Mae mwy o waith i'w wneud i wireddu hyn. Bydd camau tymor byr yn cynnwys: (i) sefydlu Bwrdd Cynghori Seiber Cenedlaethol newydd, gan wahodd uwch arweinwyr o'r sector preifat a'r trydydd sector i herio, cefnogi a chyfrannu at ein dull gweithredu; (ii) ailgyfeirio ein rhaglenni arloesi yn y sector seiber oddi wrth fentrau mawr, sy'n aml yn Llundain i fodel sy'n cael ei ddarparu'n rhanbarthol, wedi'i adeiladu mewn partneriaeth â diwydiant lleol, arloeswyr, asiantaethau gorfodi'r gyfraith a'r byd academaidd; a (iii) cymryd camau i gynyddu amrywiaeth y gweithlu seiber – gan gydnabod bod gallu meithrin sgiliau a doniau'r boblogaeth gyfan yn hanfodol ar gyfer ein diogelwch cenedlaethol. Mae'r strategaeth ei hun wedi cael ei llywio gan ymgysylltu â llywodraethau datganoledig Cymru, Gogledd Iwerddon a'r Alban, diwydiant, asiantaethau gorfodi'r gyfraith, rheoleiddwyr, y byd academaidd, cymdeithas sifil a phartneriaid rhyngwladol. Ein bwriad yw cadw'r deialogau hyn yn agored dros y cyfnod gweithredu.

52. Dull mwy rhagweithiol o faethu a diogelu ein mantais gystadleuol yn y technolegau sy'n hanfodol i seiberofod. Mae'r Adolygiad Integredig a'r strategaethau dilynol eisoes wedi dechrau bwrw ymlaen â'r dull gweithredu hwn mewn meysydd fel deallusrwydd artiffisial, technolegau cwantwm a data. Mae'r strategaeth hon yn gwneud ymrwymiadau pellach ynghylch dylunio microbrosesyddion diogel, diogelwch technolegau gweithredol a chryptograffeg. Mae'n cyhoeddi sefydlu labordy cenedlaethol ar gyfer diogelwch technoleg weithredol, fel canolfan ragoriaeth newydd sy'n canolbwyntio ar feithrin y lefel uchaf o seibergadernid mewn partneriaeth â diwydiant a'r byd academaidd. Ac mae'n cyhoeddi ehangu galluoedd ymchwil y Ganolfan Seiberddiogelwch Genedlaethol (NCSC), gan gynnwys y ganolfan ymchwil gymhwysol newydd ym Manceinion, gan ganolbwyntio ar dechnoleg newydd mewn meysydd fel trafnidiaeth a mannau cysylltiedig. Mae'r strategaeth hefyd yn adeiladu ar ein gwaith llwyddiannus i hyrwyddo dulliau sy'n ymgorffori diogelwch mewn technolegau newydd, gan eu gwneud yn "ddiogel drwy ddylunio". Bydd hyn yn golygu buddsoddi a gwneud mwy o ddefnydd o ysgogiadau rheoleiddiol a deddfwriaethol lle bo angen i hyrwyddo cadwyni cyflenwi technoleg mwy amrywiol, diogel a chadarn, fel rydym wedi'i wneud ym maes telathrebu.

53. Cryfhau ein hymdrech graidd yn sylweddol i hyrwyddo seiberddiogelwch, gyda'r llywodraeth yn arwain y ffordd. Byddwn yn buddsoddi mwy nag erioed o'r blaen mewn ailwampio seiberddiogelwch y llywodraeth yn gyflym ac yn radical, gan osod safonau clir ar gyfer adrannau a mynd i'r afael â hen seilwaith TG. Bydd y gallu sydd gan swyddogaethau craidd llywodraeth i wrthsefyll ymosodiadau seiber yn cael ei gryfhau'n sylweddol erbyn 2025, a byddwn yn sicrhau bod holl sefydliadau'r llywodraeth – ar draws y sector cyhoeddus – yn gallu gwrthsefyll gwendidau a dulliau ymosod hysbys erbyn 2030. Byddwn yn gwneud mwy i amddiffyn ac ymgysylltu â dinasyddion gan gael gwared â chymaint o'r baich oddi arnynt ag sy'n bosibl. Byddwn yn caledu'r amgylchedd digidol, gan ddiogelu dinasyddion rhag seiberdroseddu a thwyll a rhoi mwy o gyfrifoldeb ar wneuthurwyr, adwerthwyr, darparwyr gwasanaethau a'r sector cyhoeddus i godi safonau seiberddiogelwch. Byddwn yn cynyddu lefel ymgysylltiad a buddsoddiad y sector preifat mewn seibergadernid drwy gysoni rheoliadau a chymhellion ar draws yr economi a darparu mwy o gymorth. Byddwn hefyd yn canolbwyntio mwy ar risgiau'r gadwyn gyflenwi, gan brofi amrywiaeth o ymyriadau i helpu sefydliadau i reoli'r risgiau seiberddiogelwch gan eu cyflenwyr, a sicrhau bod arferion gorau yn treiddio i lawr drwy'r gadwyn gyflenwi.

54. Ymgyrchoedd mwy integredig a pharhaus i amharu ar ein gwrthwynebwyr a'u hatal a diogelu a hyrwyddo buddiannau'r DU mewn seiberofod. Bydd yr ymgyrchoedd hyn yn defnyddio ystod lawnach o ysgogiadau gweithredol, polisi a diplomyddol ar draws y llywodraeth. Byddant yn cael eu hategu'n sylweddol drwy sefydlu ac ehangu'r Llu Seiber Cenedlaethol (NCF), a leolir yn Samlesbury yn Swydd Gaerhirfryn. Byddwn yn gwneud defnydd mwy rheolaidd o alluoedd yr NCF i ymyrryd â bygythiadau gan weithredwyr gwladwriaethol ac anwladwriaethol ac i gefnogi buddiannau diogelwch gwladol ehangach y DU. Bydd ein hymgyrchoedd hefyd yn elwa o fuddsoddiad newydd mawr mewn galluoedd o'r radd flaenaf ar gyfer gorfodi'r gyfraith ar lefel genedlaethol, ranbarthol a lleol. Bydd hyn yn ein helpu i fynd i'r afael â'r bygythiad sylweddol o feddalwedd wystlo a seiberdroseddwyr sy'n dod yn fwy ac yn fwy arloesol. Byddwn hefyd yn parhau i ddefnyddio trefn sancsiynau seiber ymreolaethol y DU a'r broses briodoli i osod costau ar ein gwrthwynebwyr a thynnu sylw at ymosodiadau niweidiol a di-hid.

55. Rhoi pŵer seiber wrth galon agenda polisi tramor y DU a chydnabod bod angen ymgysylltu rhyngwladol ar gyfer pob rhan o'r strategaeth. Byddwn yn atgyfnerthu ein cynghreiriau craidd ac yn ymgysylltu ag ystod ehangach o wledydd i wrthsefyll ymlediad awdurdodyddiaeth ddigidol. Dros y blynyddoedd nesaf, byddwn yn cynyddu'r buddsoddiad mewn rhaglenni rhyngwladol i gefnogi gwledydd partner, gan helpu i feithrin eu gwytnwch a gwella eu gallu i wrthsefyll bygythiadau seiber. A byddwn yn defnyddio ystod lawn ein cryfderau domestig yn well, gan gynnwys arbenigedd cyfathrebu gweithredol a strategol, arwain agweddau, perthnasoedd masnachu a phartneriaethau diwydiannol i gefnogi ein nodau rhyngwladol.

Rolau a chyfrifoldebau ar draws y DU

56. Bydd dull gweithredu cymdeithas gyfan ar gyfer seiber yn ganolog i'n strategaeth. Mae angen i ni adeiladu partneriaeth barhaus a chytbwys ar draws y sector cyhoeddus, y sector preifat a'r trydydd sector, gyda phob un yn chwarae rhan bwysig yn ein hymdrech genedlaethol.

Dinasyddion

57. Mae'r strategaeth hon yn ceisio dileu cymaint â phosibl o'r baich seiberddiogelwch oddi ar ddinasyddion, ond byddwn i gyd yn parhau i fod â rhan bwysig i'w chwarae. Er y bydd y llywodraeth yn gwneud cymaint â phosibl i atal ymosodiadau seiber cyn iddynt achosi niwed i bobl, bydd rhai gweithredwyr bygythiadau yn dod o hyd i ffordd o osgoi'r amddiffyniadau hyn. Gall pob un ohonom gymryd camau i wella diogelwch yr asedau rydym yn eu gwerthfawrogi yn y byd ffisegol a'r byd rhithwir.[20] Mae hynny'n golygu cyflawni ein cyfrifoldeb personol i gymryd pob cam rhesymol i ddiogelu nid yn unig ein caledwedd – ein ffonau clyfar a'n dyfeisiau eraill – ond hefyd y data, y meddalwedd a'r systemau sy'n rhoi rhyddid, hyblygrwydd a hwylustod i ni yn ein bywydau preifat a phroffesiynol. I gefnogi hyn, mae'r llywodraeth yn darparu cyngor technegol cywir, amserol y gellir gweithredu arno. Mae sefydliadau cymdeithas sifil a grwpiau cymunedol hefyd yn chwarae rhan bwysig drwy gefnogi pobl i ddeall a diogelu eu hunain rhag risgiau seiber. Mae llawer o elusennau, er enghraifft, yn darparu cefnogaeth wedi'i thargedu, cyngor a chodi ymwybyddiaeth i grwpiau agored i niwed.

[20] Cyber Aware yw cyngor y llywodraeth ar sut i gadw'n ddiogel ar-lein

Busnesau a sefydliadau

58. Mae gan fusnesau a sefydliadau gyfrifoldeb i sicrhau eu bod yn rheoli eu risgiau seiber yn effeithiol, i fod yn seibergadarn ac i gefnogi eu cwsmeriaid a'r bobl sy'n defnyddio eu gwasanaethau. Mae busnesau a sefydliadau'n dibynnu fwyfwy ar dechnolegau digidol a gwasanaethau ar-lein i weithredu, i arloesi ac i dyfu. Mae hyn yn gwella gwasanaethau ond mae hefyd yn creu risgiau a heriau newydd, fel y cynnydd parhaus mewn faint o ddata personol ac asedau digidol maen nhw'n gyfrifol amdanynt. Daw hyn â chyfrifoldeb i ddiogelu'r data a'r asedau hynny, gan gynnal gwasanaethau ar yr un pryd. Gall methu â gwneud hynny arwain at oblygiadau sylweddol i enw da ac yn economaidd i sefydliadau ac achosi niwed i'w cwsmeriaid. Mae gan weithredwyr gwasanaethau hanfodol a darparwyr gwasanaethau digidol allweddol (fel gwasanaethau yn y cwmwl) gyfrifoldebau penodol i fynd i'r afael â'r risgiau seiber maen nhw'n eu hwynebu ac i gyflawni'r rhwymedigaethau sydd wedi'u nodi yn Rheoliadau Rhwydweithiau a Systemau Gwybodaeth ('rheoliadau NIS'). Mae cyngor ac arweiniad gan yr NCSC yn helpu i ddarparu cymorth i bob busnes a sefydliad i'w helpu i ddiogelu eu gwybodaeth, eu hasedau a'u systemau. Mae Swyddfa'r Comisiynydd Gwybodaeth (ICO) hefyd yn rhoi cyngor i sefydliadau ar eu rhwymedigaethau seiberddiogelwch o dan Reoliad Cyffredinol y DU ar Ddiogelu Data.

Y sector seiberddiogelwch a chwmnïau technoleg mawr

59. Mae gan y sector seiberddiogelwch sy'n tyfu yn y DU rôl hollbwysig o ran ymateb i'r bygythiadau seiber a'r heriau sy'n wynebu ein gwlad. Mae'r cynnydd cyflym mewn dyfeisiau cysylltu a'r broses o drawsnewid busnesau a sefydliadau'n ddigidol yn gyflymach yn rhoi cyfleoedd i'r sector dyfu ac arloesi, gan ddarparu gwasanaethau a chynnyrch newydd. Mae'r strategaeth hon yn disgrifio sut bydd y llywodraeth yn parhau i gefnogi twf sector seiberddiogelwch y DU ac yn elwa o'u gallu a'u harbenigedd drwy gynnal a chryfhau ein partneriaethau. Rydym hefyd eisiau cryfhau'r partneriaethau ehangach rhwng y byd academaidd, y gymuned dechnegol ehangach a'r sector preifat, er mwyn sicrhau ein bod yn manteisio i'r eithaf ar arbenigedd technegol a gwybodaeth y DU.

60. Mae gan y prif gwmnïau technoleg sy'n darparu gwasanaethau digidol ran hollbwysig i'w chwarae o ran sicrhau amgylchedd diogel i fusnesau a sefydliadau'r DU weithredu ynddo. Mae hyn yn arbennig o wir am y darparwyr gwasanaethau a reolir a'r busnesau platfform sy'n integreiddio nifer o weithgareddau. Mae angen iddynt sicrhau bod y gwasanaethau maent yn eu cynnig yn 'ddiogel yn ddiofyn' ac nad ydynt yn dibynnu gormod ar fod eu cwsmeriaid yn cymryd camau amddiffynnol. Mae gan gwmnïau technoleg mawr gyfrifoldeb penodol hefyd i flaenoriaethu eu seibergadernid eu hunain. Mae dibyniaeth gynyddol busnesau, y llywodraeth a'r gymdeithas ehangach ar wasanaethau cwmwl ac ar-lein yn creu gwendidau a rhyngddibyniaethau newydd ac unigryw.

Llywodraeth

61. Mae **Llywodraeth y DU** mewn sefyllfa unigryw i ddod â'r gudd-wybodaeth angenrheidiol at ei gilydd i ddeall y bygythiadau mwyaf soffistigedig, i greu ac i orfodi'r gyfraith, i osod safonau cenedlaethol, ac i wrthsefyll bygythiadau gan weithredwyr gelyniaethus, gan gynnwys cynnal ymgyrchoedd seiber ymosodol. Drwy'r strategaeth hon byddwn yn buddsoddi i gryfhau ein galluoedd seiber cenedlaethol. Mae adrannau'r llywodraeth a chyrff y sector cyhoeddus hefyd yn gyfrifol am ddiogelu eu rhwydweithiau a'u systemau eu hunain. Fel deiliad data sylweddol a darparwr gwasanaethau, mae'r llywodraeth yn cymryd camau llym i ddarparu mesurau diogelu ar gyfer ei hasedau gwybodaeth. Yn olaf, mae gan y llywodraeth hefyd gyfrifoldeb pwysig i gynghori a rhoi gwybod i ddinasyddion, i fusnesau ac i sefydliadau beth mae angen iddynt ei wneud i ddiogelu eu hunain ar-lein. Lle bo angen, mae hyn yn cynnwys gosod y safonau rydym yn disgwyl i gwmnïau a sefydliadau allweddol eu bodloni er mwyn amddiffyn pob un ohonom.

62. Mae'r rhan fwyaf o feysydd polisi seiber a'r rhan fwyaf o'r mesurau a amlinellir yn y strategaeth hon yn ymwneud â materion a gedwir yn ôl fel diogelwch gwladol, materion tramor ac amddiffyn, telegyfathrebu, safonau cynnyrch a diogelwch, a diogelu defnyddwyr. Ond mae datblygu a gweithredu'r strategaeth hon yn dal i ddibynnu ar fewnbwn, camau gweithredu a buddsoddiad gan **lywodraethau datganoledig Cymru, Gogledd Iwerddon a'r Alban**. Mae hyn yn arbennig o wir lle mae hyn yn ymwneud â meysydd polisi datganoledig sy'n gorwedd yn bennaf o fewn colofnau 'ecosystem' a 'chadernid' y strategaeth hon, fel addysg, plismona a seibergadernid rhai sectorau allweddol gan gynnwys eu sectorau cyhoeddus eu hunain. Mae cydlynu a chydweithredu ar draws pedair gwlad y DU yn hanfodol er mwyn sicrhau'r effaith fwyaf ar draws y wlad i gyd. Mae hyn yn golygu bod angen i Swyddfa'r Cabinet ac adrannau eraill llywodraeth y DU ymgysylltu'n rheolaidd ac yn gynnar â'u cymheiriaid yng Nghymru, yr Alban a Gogledd Iwerddon er mwyn rhannu gwybodaeth am flaenoriaethau a chynlluniau. Mae hyn hefyd yn helpu i osgoi dyblygu a chael y gwerth gorau o gyllid cyhoeddus. Bydd y llywodraethau datganoledig yn dal i ddatblygu eu strategaethau a'u cynlluniau seiber eu hunain, gan eu cysoni â'r strategaeth hon gan lywodraeth y DU.

Y Ganolfan Seiberddiogelwch Genedlaethol

"Helpu i wneud y DU y lle mwyaf diogel i fyw a gweithio ar-lein"

Cafodd y Ganolfan Seiberddiogelwch Genedlaethol (NCSC) ei lansio'n ffurfiol yn 2017, fel rhan o Bencadlys Cyfathrebu Llywodraeth y DU, i fod yn awdurdod cenedlaethol y DU ar yr amgylchedd seiberddiogelwch: rhannu gwybodaeth, mynd i'r afael â gwendidau systemig a darparu arweinyddiaeth ar faterion seiberddiogelwch cenedlaethol allweddol.[21] Roedd sefydlu'r NCSC wedi symleiddio strwythurau gweithredol y llywodraeth, wedi trawsnewid gallu'r DU i ymateb i ddigwyddiadau seiber ar lefel genedlaethol, ac wedi dechrau cyflwyno gwasanaethau digidol arloesol sydd wedi helpu i wneud sefydliadau ac unigolion yn fwy diogel ar-lein yn awtomatig.

Rydym yn gwneud yn siŵr bod yr NCSC yn addas ar gyfer heriau'r degawd nesaf drwy egluro'r galluoedd a'r priodoleddau parhaus sy'n sail i'w gwaith, eu hariannu ar sail gynaliadwy, a chanolbwyntio ar eu defnydd pan fydd y profiad o'u gweithredu hyd yma yn dweud wrthym y byddant yn cael yr effaith fwyaf bosibl ar raddfa genedlaethol.

Dyma'r galluoedd a'r priodoleddau parhaus sy'n sail i waith yr NCSC:

- Arbenigedd technegol o'r radd flaenaf yn y disgyblaethau a'r arbenigeddau seiberddiogelwch sydd eu hangen ar y DU;
- Dealltwriaeth ddigyffelyb o fygythiadau seiber presennol a phosibl – bwriad a gallu – i fuddiannau'r DU;
- Mynediad at yr ystod lawn o awdurdodau a galluoedd diogelwch cenedlaethol y DU ar gyfer nodau seiberddiogelwch;
- Cysylltu'n uniongyrchol â chymunedau seiberddiogelwch ar y cyd â phartneriaid yn y byd academaidd, diwydiant ac yn rhyngwladol;
- Gwasanaethau a galluoedd cryptograffig, sy'n hanfodol i ddiogelwch a diogelwch buddiannau'r DU yn fyd-eang.

Prif gyfrifoldebau'r NCSC dan y strategaeth newydd fydd:

- **Cymryd camau uniongyrchol i leihau niwed seiber i'r DU** drwy ddarparu amddiffyniad ar raddfa fawr drwy wasanaethau digidol (ee Active Cyber Defence), sbarduno newidiadau mewn technoleg, rheoli'r ymateb i ddigwyddiadau seiber sy'n arwyddocaol yn genedlaethol, a – gyda'r Llu Seiber Cenedlaethol (NCF) – mynd i'r afael yn uniongyrchol â gweithrediadau seiber ein gwrthwynebwyr.

[21] Llywodraeth Ei Mawrhydi, National Cyber Security Strategy 2016 to 2021 (2016): paragraff 1.9

- **Cefnogi pob rhan o gymdeithas y DU i amddiffyn eu hunain** drwy ddarparu arbenigedd wedi'i deilwra a gwybodaeth unigryw y gall dinasyddion, busnesau a sefydliadau ledled y DU ei defnyddio i amddiffyn eu hunain a helpu i wneud y DU yn lle mwy diogel i bawb ar-lein.
- **Darparu mewnbwn technegol i bolisïau a rheoliadau Llywodraeth Ei Mawrhydi ar y materion pwysicaf ar gyfer seiberddiogelwch** drwy ddarparu mewnbwn technegol ac asesiad awdurdodol o fygythiadau i arweinwyr polisi ar draws Whitehall sy'n deillio o alluoedd craidd yr NCSC, gan gefnogi'r gwaith o ddatblygu a gweithredu polisïau a rheoliadau i gadw dinasyddion, sefydliadau a buddiannau'r DU yn ddiogel yn ddigidol.
- **Darparu galluoedd sofran y DU** drwy Ganolfan Crypt-Allwedd Genedlaethol yr NCSC, sy'n diogelu'r wybodaeth a'r gwasanaethau hanfodol y mae cymuned diogelwch genedlaethol a milwrol y DU yn dibynnu arnynt, gan gynnwys rhag ymosodiad gan ein gwrthwynebwyr mwyaf galluog.
- **Cefnogi twf mewn buddsoddi a sgiliau seiber** drwy ddarparu'r sylfaen dechnegol ar gyfer pob lefel o addysg seiber ac ymgysylltu â'r diwydiant a'i gefnogi, gan ysgogi buddsoddiad yn y sector seiber.

Bydd yr NCSC hefyd yn cyfrannu at **werthuso cynnydd** yn erbyn amcanion y strategaeth seiber genedlaethol hon drwy Asesiadau NCSC, swyddogaeth asesiadau seiber sy'n olygyddol annibynnol y DU.

Y Llu Seiber Cenedlaethol

Cafodd y Llu Seiber Cenedlaethol (NCF) ei sefydlu yn 2020, ac mae'n gyfrifol am weithredu mewn seiberofod a drwyddo i wrthsefyll, tarfu, diraddio a chystadlu yn erbyn y rheini a fyddai'n gwneud niwed i'r DU neu ei chynghreiriaid, i gadw'r wlad yn ddiogel ac i ddiogelu ac i hyrwyddo buddiannau'r DU gartref a thramor. Mae'r NCF yn cynnwys cyfran gweddol gyfartal o staff o amddiffyn a chudd-wybodaeth ac mae'n dwyn ynghyd eu harbenigedd, eu hadnoddau a'u hawdurdodau dan un strwythur gorchymyn. Mae wedi'i leoli yn Samlesbury, Swydd Gaerhirfryn.

Mae'r NCF yn darparu amrywiaeth eang o ganlyniadau er budd diogelwch gwladol, fel cymorth i amddiffyn, lles economaidd y DU ac atal troseddau difrifol. Mae gweithgareddau'r NCF yn amrywio, o'r tactegol i'r strategol, yn erbyn gweithredwyr gwladwriaethol a gweithredwyr anwladwriaethol. Mae ei waith yn perthyn i dri phrif gategori:

- Mynd i'r afael â bygythiadau gan derfysgwyr, troseddwyr a gwladwriaethau sy'n defnyddio'r rhyngrwyd i weithredu ar draws ffiniau er mwyn gwneud niwed i'r DU ac i gymdeithasau democrataidd eraill
- Mynd i'r afael â bygythiadau sy'n amharu ar gyfrinachedd, cywirdeb ac argaeledd data a gwasanaethau mewn seiberofod (hy cefnogi seiberddiogelwch)
- Cyfrannu at weithrediadau Amddiffyn y DU a helpu i gyflawni agenda polisi tramor y DU (er enghraifft ymyrryd mewn argyfwng dyngarol i amddiffyn dinasyddion)

Gellir defnyddio gweithrediadau'r NCF i ddylanwadu ar unigolion a grwpiau, tarfu ar systemau cyfathrebu ac ar-lein a diraddio gweithrediadau systemau ffisegol. Cyfeirir yn aml at y math hwn o weithgaredd fel seiber ymosodol (OC).

Mae gweithrediadau'r NCF yn cael eu cynnal yn unol â fframwaith cyfreithiol sydd wedi hen ennill ei blwyf, sy'n cynnwys Deddf Gwasanaethau Cudd-wybodaeth 1994 a Deddf Pwerau Ymchwilio 2016. Mae'r DU wedi datgan yn glir o'r blaen ei bod yn datblygu ac yn defnyddio galluoedd yn unol â chyfraith ryngwladol, gan gynnwys cyfraith gwrthdaro arfog lle bo hynny'n berthnasol. Mae ei weithgareddau'n amodol ar gymeradwyaeth weinidogol, goruchwyliaeth farnwrol ac adolygiad seneddol, sy'n golygu mai trefn lywodraethu'r DU ar gyfer gweithrediadau seiber yw un o'r cryfaf yn y byd.

Fel mater o drefn ni fydd y DU yn siarad am weithrediadau seiber unigol, ond mae'r mathau o weithgarwch gweithredol y gallai'r NCF eu cynnal yn cynnwys:

- Stopio grwpiau terfysgol rhag cyflawni eu cynlluniau drwy analluogi eu cyfathrebiadau gorchymyn a rheoli a chyfyngu ar ledaenu cyfryngau eithafol
- Lleihau'r risg o niwed i luoedd arfog y DU drwy ddiraddio systemau arfau gwrthwynebwyr
- Amddiffyn democratiaeth ac etholiadau rhydd, teg ac agored drwy fynd i'r afael ag ymgyrchoedd twyllwybodaeth camarweiniol sy'n cael eu trefnu gan y wladwriaeth i geisio tanseilio'r etholiadau hynny
- Atal grwpiau troseddol rhag elwa o'u gweithgareddau drwy amharu ar eu defnydd o blatfformau a gwasanaethau ar-lein
- Helpu i orfodi sancsiynau rhyngwladol drwy amharu ar ymdrechion i'w hosgoi
- Gwarchod y DU ac eraill rhag ymosodiadau seiber drwy amharu ar y seilwaith a ddefnyddir gan wrthwynebwyr i'w cyflawni
- Amddiffyn dinasyddion mewn argyfwng dyngarol drwy gadw eu gallu i gael gafael ar wybodaeth hanfodol

Fel y ganolfan rhagoriaeth genedlaethol ar gyfer gweithrediadau effeithiau mewn seiberofod a drwyddo, bydd yr NCF yn trawsnewid gallu'r DU i ddatblygu, integreiddio a defnyddio'r galluoedd hyn ochr yn ochr ag eraill a'u hoptimeiddio i gyflawni'r effaith.

Rhwydwaith Seiberdroseddu Cenedlaethol Asiantaethau Gorfodi'r Gyfraith

Wedi'i sefydlu yn ystod Strategaeth Seiberddiogelwch Genedlaethol 2016-2021, mae rhwydwaith seiberddiogelwch cenedlaethol asiantaethau gorfodi'r gyfraith wedi datblygu ymateb cwbl integredig i seiberdroseddu, sy'n barod i ddarparu ymateb sy'n seiliedig ar gudd-wybodaeth i bob math o ymosodiadau seiber yn erbyn unigolion, sefydliadau neu sectorau cyfan. Mae hon yn system genedlaethol sy'n gweithredu ar lefel genedlaethol, ranbarthol a lleol. Mae'n darparu gofal i ddioddefwyr, yn helpu busnesau a phobl i gael eu hamddiffyn ac adfer yn gyflym, ac yn mynd ar drywydd canlyniadau cyfiawnder troseddol yn erbyn drwgweithredwyr.

Mae **Uned Seiberdroseddu Genedlaethol (NCA) yr Asiantaeth Troseddu Cenedlaethol (NCCU)** yn darparu arweinyddiaeth genedlaethol ac yn cydlynu'r ymateb, gyda rhwydwaith o **Unedau Seiberdroseddu Rhanbarthol (RCCUs)** pwrpasol ym mhob un o naw rhanbarth heddlu Cymru a Lloegr, mewn partneriaeth â'u cymheiriaid yn yr Heddlu yn yr Alban a Gwasanaeth Heddlu Gogledd Iwerddon, yn ogystal ag Uned Seiberdroseddu'r Gwasanaeth Heddlu Metropolitanaidd.

Mae'r rhain yn cael eu hategu ymhellach gan **Unedau Seiberdroseddu Lleol (LCCUs)** penodol, wedi'u gwreiddio ym mhob un o'r 43 heddlu ac wedi'u cysoni drwy gydlynydd rhanbarthol. Mae'r CCUs Rhanbarthol a Lleol hyn yn gallu ymchwilio i droseddwyr a mynd ar eu trywydd, helpu busnesau a dioddefwyr i amddiffyn eu hunain rhag ymosodiadau a gweithio gyda phartneriaid i atal unigolion agored i niwed rhag cael eu denu i seiberdroseddu.

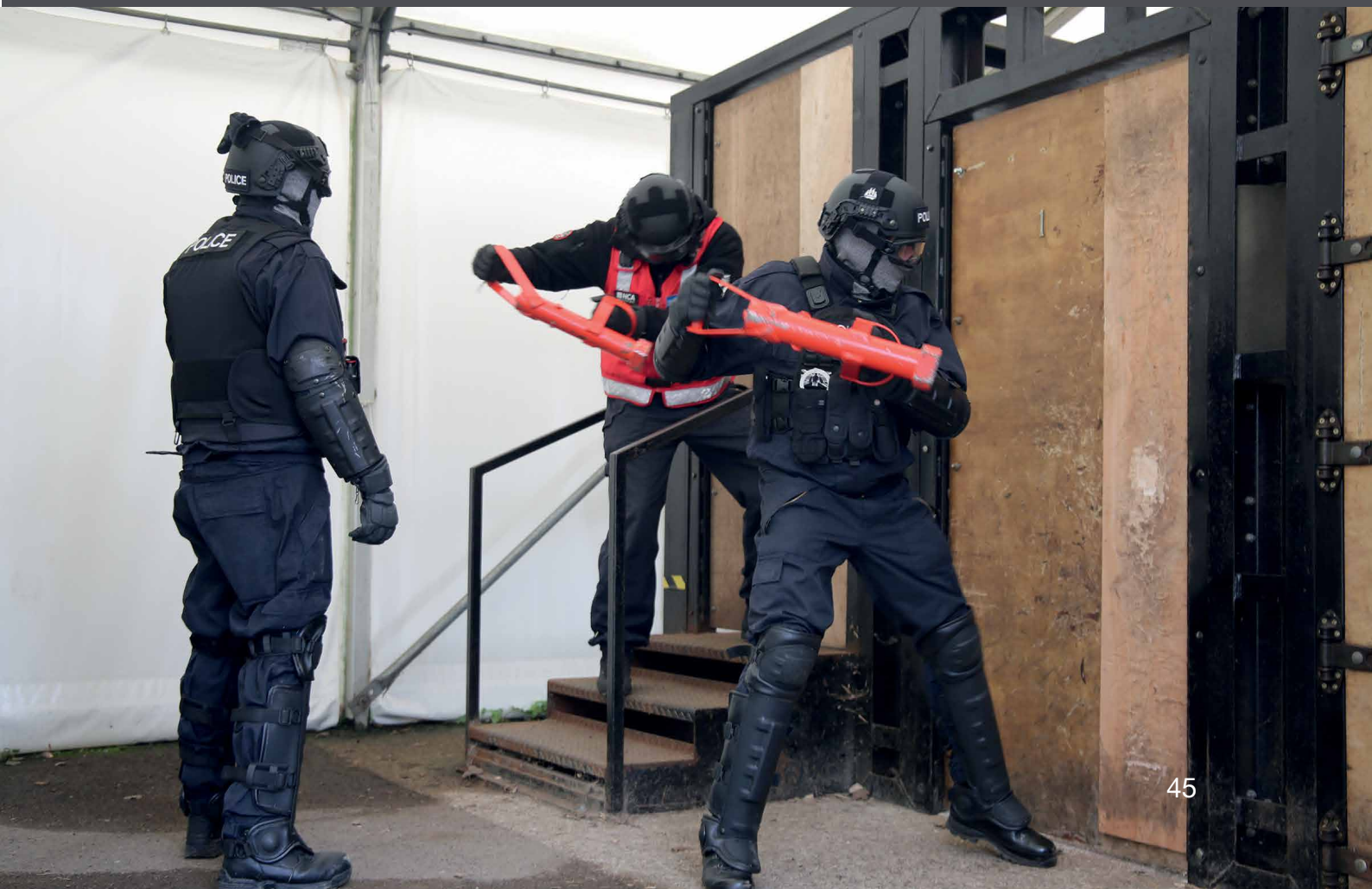
Mae riportio, blaenoriaethu a dadansoddi troseddau yn ganolog yn cael ei wneud drwy **Action Fraud**, sy'n cael ei gynnal gan **Heddlu Dinas Llundain**. Mae'r achosion mwyaf difrifol a/neu gymhleth yn cael eu cyfeirio wedyn at yr NCA a'r rhwydwaith rhanbarthol i'w dilyn, tra bo achosion eraill yn cael eu dosbarthu i heddluoedd lleol. Mae Heddlu Dinas Llundain hefyd yn cydlynu cymorth i ddioddefwyr, gan gynnwys drwy'r **Uned Gofal i Ddioddefwyr am Droseddau Economaidd**.

Mae systemau'n cael eu cysylltu â galluoedd fforensig, cudd-wybodaeth a rhannu data sydd wedi'u gweddnewid er mwyn creu un platfform i unedau cenedlaethol a rhanbarthol allu cael gafael ar yr holl adnoddau a galluoedd lefel uchel arbenigol sy'n cael eu datblygu. Mae hyn yn cynnwys y gallu i gydweithio'n effeithiol â phartneriaid yn y gymuned ddiogelwch a chudd-wybodaeth, yn enwedig i ymateb i fygythiadau cyfunol gan droseddwyr a gwladwriaethau. Gan barhau â'r ethos

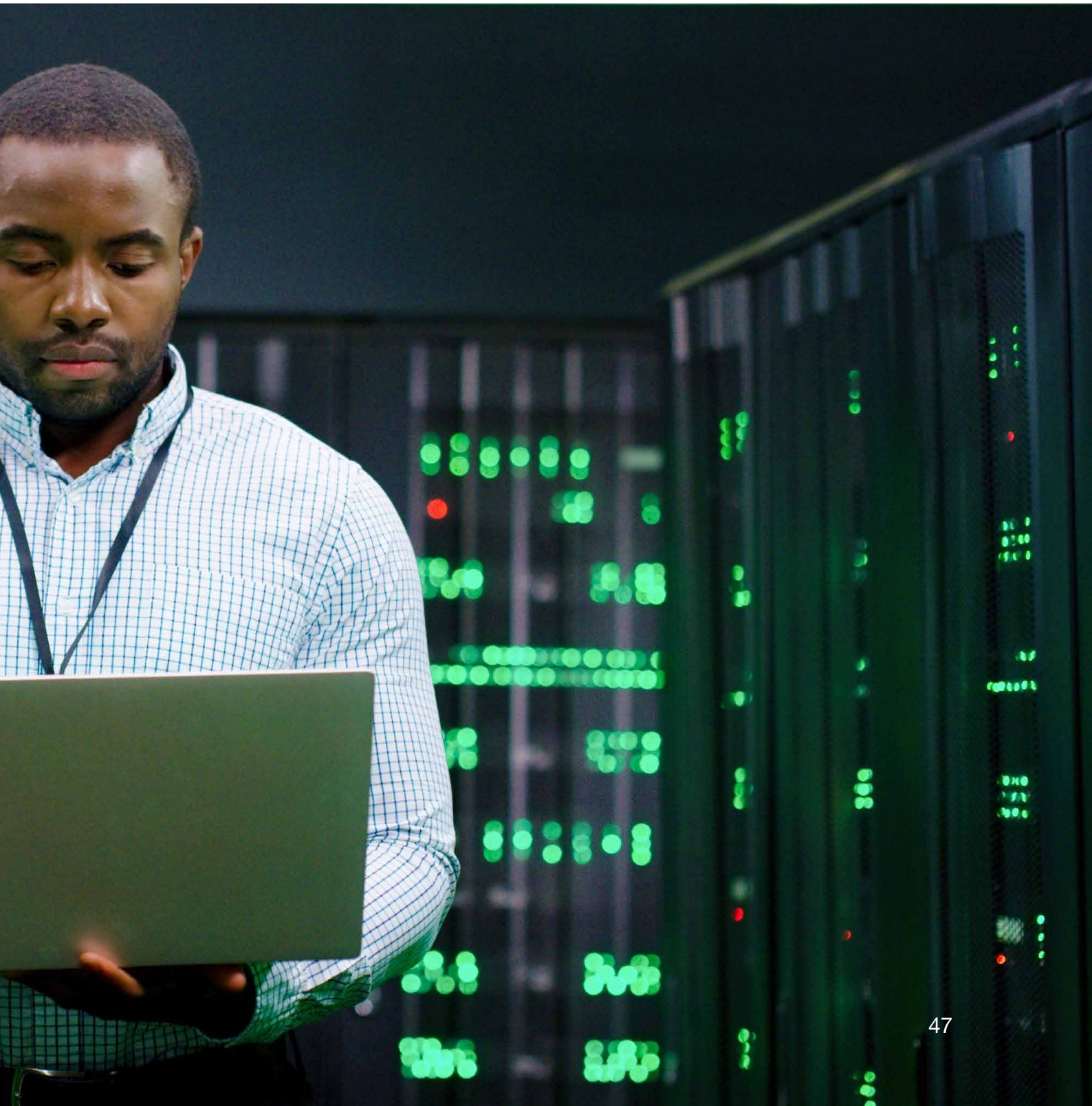
o ‘ei adeiladu unwaith, ei adeiladu’n genedlaethol er budd y rhwydwaith seiberdroseddu cyfan’, mae modd i’r unedau seiberdroseddu lleol gael mynediad at y galluoedd hyn hefyd drwy’r cydlynwyr rhanbarthol. Mae’r dull system gyfan hwn eisoes yn darparu ymateb llawer gwell i’r bygythiad o seiberdroseddu.

Bydd Rhwydwaith Seiberdroseddu asiantaethau gorfodi’r gyfraith yn dal i yrru ein hymateb cyfiawnder troseddol i weithgareddau maleisus mewn seiberofod, dim ots pwy sydd y tu ôl i’r bygythiad ar lefel ryngwladol, genedlaethol, ranbarthol a lleol. Ategir hyn gan amrywiaeth o ddulliau eraill sy’n tarfu gan gynnwys y canlynol, ond nid dim ond y rhain:

- Datblygu galluoedd ymchwilio a tharfu arbenigol o’r radd flaenaf
- Defnyddio rhwydwaith rhyngwladol helaeth yr NCA i gefnogi ymyriadau gwledydd partner gyda chudd-wybodaeth a thystiolaeth
- Atal grwpiau troseddol rhag elwa o’u gweithgareddau drwy amharu ar eu defnydd o farchnadoedd troseddol a gwasanaethau sy’n cael eu galluogi
- Amddiffyn y DU a gwledydd eraill rhag seiberdroseddau drwy ddiraddio ac amharu ar y seilwaith a ddefnyddir i’w cyflawni
- Cyfrannu at weithgarwch sy’n ymwneud â sancsiynau a phriodoli i’r cyhoedd yn erbyn troseddwyr sydd ar lefelau uchel iawn
- Meddiannu cryptoarian ac asedau eraill fel elw seiberdroseddau



Rhan 2:
Gweithredu



Colofn 1:

Ecosystem Seiber y DU

Cryfhau ecosystem seiber y DU

63. Er mwyn i'r strategaeth hon lwyddo mae angen i ni sicrhau bod gan y DU y bobl, y wybodaeth a'r partneriaethau cywir. Mae'n rhaid i ni gael gweithlu amrywiol sy'n meddu ar sgiliau technegol, cymuned ymchwil fywiog, sector seiber sy'n gystadleuol yn rhyngwladol ac ecosystem arloesi ranbarthol ffyniannus sy'n ein galluogi i gymryd yr awenau gyda thechnolegau hanfodol, ac mae pob un yn seiliedig ar bartneriaethau cryfach rhwng y llywodraeth, y diwydiant a'r byd academaidd.

64. Mae angen i dwf yr ecosystem seiber fod yn hunangynhaliol, nid yn ddibynnol ar ymyriadau'r llywodraeth. Yn ystod y strategaeth hon, byddwn yn symud o gyllido amrywiaeth o raglenni sgiliau ac arloesedd pwrpasol sy'n cael eu rheoli'n ganolog yn bennaf, i ddull gweithredu mwy cynaliadwy, systemig a rhanbarthol. Byddwn yn adeiladu ar ddiwygiadau ehangach y llywodraeth i'r systemau sgiliau ac addysg i gefnogi ac i ysbrydoli rhagor o bobl i ennill y sgiliau sydd eu hangen arnynt i ddilyn gyrfa seiber. A byddwn yn blaenoriaethu amrywiaeth o gamau gweithredu pendant i gynyddu amrywiaeth y gweithlu seiber. Mae hyn yn ymwneud â sicrhau bod y swyddi a'r gyrfaoedd hyn ar gael i bawb ond mae hefyd yn hanfodol i'n diogelwch cenedlaethol, gan sicrhau ein bod yn harneisio talent a sgiliau'r boblogaeth gyfan. Byddwn hefyd yn sicrhau bod twf y sector seiber o fudd i'r DU gyfan, nid dim ond Llundain a De Ddwyrain Lloegr. Amcangyfrifir bod 45% o gyflogaeth y sector a 85% o'r buddsoddiad allanol yn perthyn i'r un ardal hon.[22]

65. At ei gilydd, byddwn yn ymgymryd â rôl fwy strategol lle rydym yn hwyluso dod ag arweinwyr y diwydiant, academyddion, arloeswyr, asiantaethau gorfodi'r gyfraith, y gymuned ddiogelwch genedlaethol ac eraill at ei gilydd sydd eisiau cydweithio i wneud y DU yn fwy cadarn yn erbyn bygythiadau seiber. Byddwn yn cysoni holl ysgogiadau'r llywodraeth i gefnogi'r ecosystem seiber, o sut mae seiber yn cael ei ddysgu mewn ysgolion i sut mae rheoliadau economaidd yn codi safonau, i sicrhau bod y DU yn tyfu'r galluoedd hanfodol sydd eu hangen i ddiogelu ein hunain yn erbyn bygythiadau yn y dyfodol.

[22] Yr Adran dros Dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon, Cyber Security Sectoral Analysis 2021 (2021)

Amcan 1: Cryfhau'r strwythurau, y partneriaethau a'r rhwydweithiau sy'n angenrheidiol i gefnogi dull gweithredu cymdeithas gyfan yng nghyswllt seiber

66. Mae pŵer seiber yn gofyn am ddull gweithredu cymdeithas gyfan. Bydd ein mantais gystadleuol yn deillio o'n gallu i feithrin a harneisio talent ledled y DU a chael y bobl iawn i weithio gyda'i gilydd yn y ffyrdd iawn ar draws y sector cyhoeddus cyfan, diwydiant a'r byd academaidd, gan ddod â'r holl gymuned seiber at ei gilydd. Bydd angen i ni greu partneriaeth gyflenwi integredig go iawn gyda'r diwydiant a sicrhau dull gweithredu daearyddol eang ar draws gwledydd a rhanbarthau'r DU, gan weithio'n agos gyda llywodraethau datganoledig Cymru, Gogledd Iwerddon a'r Alban a manteisio ar y cyfle i godi'r gwastad y mae pŵer seiber yn ei gynnig. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

67. Deialog seiber genedlaethol fwy cynhwysol a strategol gyda diwydiant, y byd academaidd a dinasyddion drwy sefydlu uwch Fwrdd Cynghori Cenedlaethol newydd ar Seiberddiogelwch, ac adeiladu ar y rhwydweithiau cadarn sydd eisoes yn bodoli o bartneriaethau cadernid a thwf seiber a'r canolfannau rhagoriaeth academaidd ar gyfer addysg ac ymchwil ym maes seiberddiogelwch.

68. Rhwydweithiau seiber rhanbarthol mwy integredig ac effeithiol ledled y DU, gan alluogi partneriaethau cryfach rhwng y llywodraeth, busnesau a'r byd academaidd i gefnogi twf sectorau a chadernid busnesau. Byddwn yn gweithio gyda chlystyrau seiber rhanbarthol a'r UK Cyber Cluster Collaboration (UKC3) a sefydlwyd yn ddiweddar, y nifer cynyddol o ganolfannau arloesi seiber rhanbarthol a Chanolfannau Seibergadernid, gan gryfhau'r cysylltiadau rhwng busnesau lleol, canolfannau rhagoriaeth academaidd ac asiantaethau gorfodi'r gyfraith.

69. Bydd y camau hyn yn adeiladu ar yr ystod o gysylltiadau presennol rhwng y Ganolfan Seiberddiogelwch Genedlaethol (NCSC) a'i rhanddeiliaid, rhwng adrannau'r llywodraeth, cyrff hyd braich a'r sectorau o'r economi maent yn eu cynrychioli, gan gynnwys CNI a rheoleiddwyr, a deialog ehangach y llywodraeth gyda'r diwydiant a'r sectorau digidol a thechnoleg.

Ciara Mitchell, Pennaeth Seiber yn ScotlandIS

Mae Ciara hefyd yn rheolwr Clwstwr Seiber yr Alban ac yn aelod o fwrdd UKC3.

“Mae Clwstwr Seiber yr Alban wedi chwarae rhan allweddol yn y gwaith o gefnogi’r gymuned seiberddiogelwch yn yr Alban. Mae dealltwriaeth gynyddol o’r arbenigedd yn yr Alban ar reoli clystyrau a’r cyfle i adeiladu ar sector seiber ffyniannus. Wrth i werth clystyrau ddod yn fwy amlwg, rwyf wedi bod yn falch iawn o ymgymryd â rôl allweddol yn y UK Cyber Cluster Collaboration newydd fel Arweinydd Datblygu Ecosystemau. Drwy UKC3 bydd mwy o ffocws ar gydweithio, arloesi a datblygu sgiliau sy’n darparu llwyfan i dyfu sector seiberddiogelwch y DU.”

Sefydliadau Seiber (Mae'r lleoliadau'n gynrychioladol)

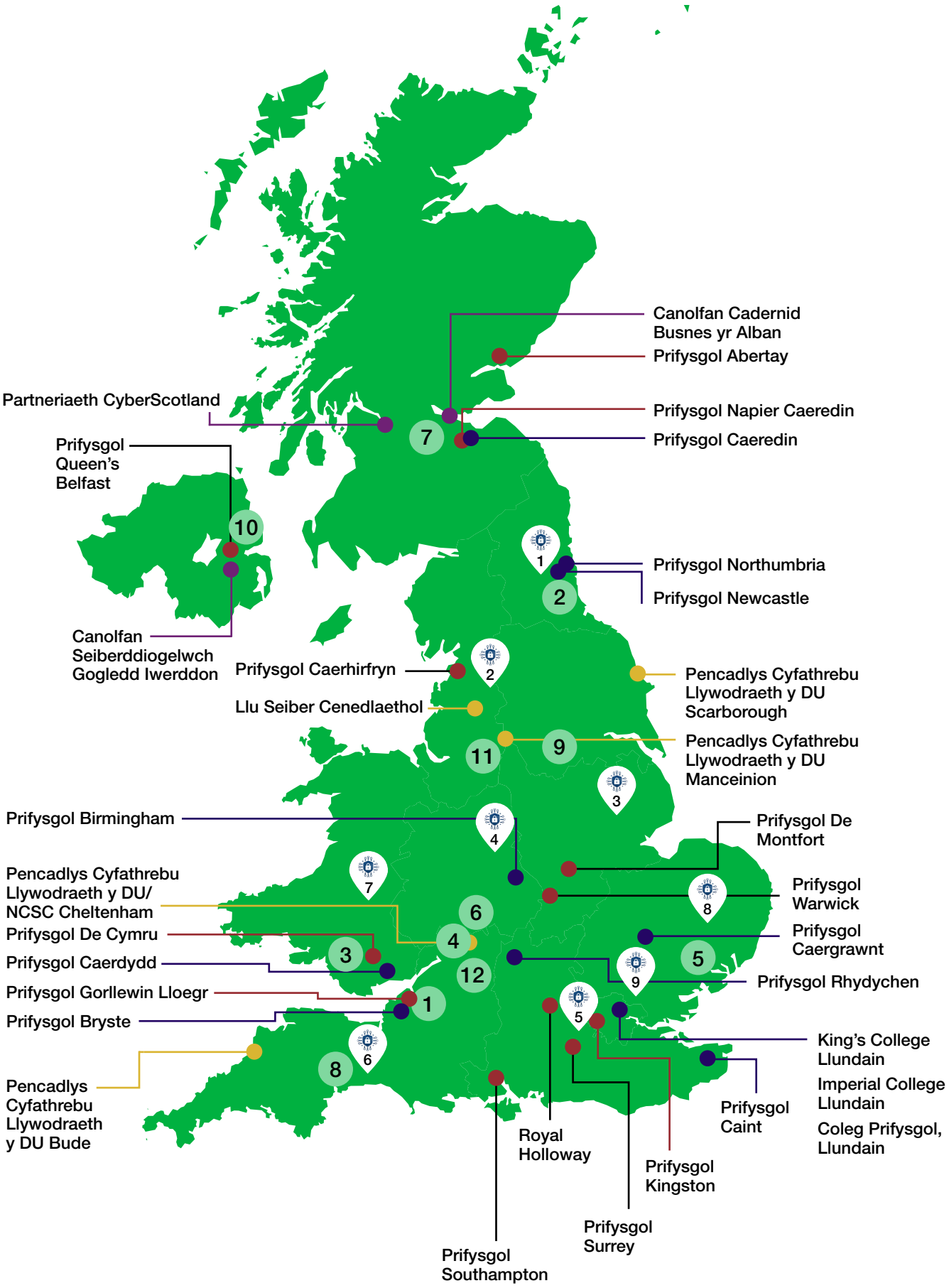
Clystyrau Seiber y DU

1. Seiber Bryste a Chaerfaddon
2. Seiber Gogledd Lloegr
3. Seiber Cymru
4. CyNam (Cyber Cheltenham)
5. Clwstwr Seiberddiogelwch Dwyrain Lloegr
6. Seiber Canolbarth Lloegr
7. Seiber ScotlandIS
8. Clwstwr Seiberddiogelwch De Orllewin Lloegr
9. Clwstwr Seiberddiogelwch Swydd Efrog
10. Seiber Gogledd Iwerddon
11. Clwstwr Seiberddiogelwch Gogledd Orllewin Lloegr
12. Clwstwr Seiber Gorllewin Lloegr

- Canolfan Ragoriaeth Academaidd mewn Addysg Seiberddiogelwch
- Safle Pencadlys Cyfathrebu Llywodraeth y DU / NCSC
- Newid Canolfan Ragoriaeth Academaidd mewn Ymchwil Seiberddiogelwch*
- Sefydliadau Awdurdodau Datganoledig

*Mae dot coch a llinell ddu yn dynodi statws CSE a CSR

1. Canolfan Cadernid Busnes Gogledd Ddwyrain Lloegr
2. Canolfan Seibergadernid Gogledd Orllewin Lloegr
3. Canolfan Seibergadernid Dwyrain Canolbarth Lloegr
4. Canolfan Seibergadernid Gorllewin Canolbarth Lloegr
5. Canolfan Seibergadernid De Ddwyrain Lloegr
6. Canolfan Seibergadernid De Orllewin Lloegr
7. Canolfan Seibergadernid Cymru
8. Canolfan Seibergadernid Dwyrain Lloegr
9. Canolfan Seibergadernid Llundain


Canolfan Cadernid Busnes yr Alban
Prifysgol Abertay
Partneriaeth CyberScotland
Prifysgol Napier Caeredin
Prifysgol Caeredin
Prifysgol Queen's Belfast
Prifysgol Northumbria
Prifysgol Newcastle
Canolfan Seiberddiogelwch Gogledd Iwerddon
Prifysgol Caerhirfryn
Pencadlys Cyfathrebu Llywodraeth y DU Scarborough
Llu Seiber Cenedlaethol
Pencadlys Cyfathrebu Llywodraeth y DU Manceinion
Prifysgol Birmingham
Prifysgol De Montfort
Pencadlys Cyfathrebu Llywodraeth y DU/ NCSC Cheltenham
Prifysgol Warwick
Prifysgol De Cymru
Prifysgol Caergrawnt
Prifysgol Caerdydd
Prifysgol Rhydychen
Prifysgol Gorllewin Lloegr
Prifysgol Bryste
King's College Llundain
Imperial College Llundain
Coleg Prifysgol, Llundain
Pencadlys Cyfathrebu Llywodraeth y DU Bude
Prifysgol Caint
Royal Holloway
Prifysgol Kingston
Prifysgol Surrey
Prifysgol Southampton

Amcan 2: Gwella ac ehangu sgiliau seiber y genedl ar bob lefel, gan gynnwys drwy broffesiwn diogelwch seiber amrywiol o safon fyd-eang sy'n ysbrydoli ac yn arfogi talent ar gyfer y dyfodol

70. Yn ganolog i uchelgais y DU fydd datblygu cyflenwad cyson ac amrywiol o bobl fedrus iawn yn y gweithlu seiber, a fydd yn gallu sicrhau elfennau craidd yr economi ddigidol, yn ogystal ag arloesi a datblygu dulliau gweithredu newydd. Bydd hyn yn cefnogi ein nod o arwain drwy esiampl drwy gydnabod a chadw arbenigedd ar draws y sector cyhoeddus a chynyddu ein gallu mewn asiantaethau gorfodi'r gyfraith, amddiffyn a diogelwch, gan gynnwys y Llu Seiber Cenedlaethol (NCF). Yn yr un modd â rhannau eraill o'r strategaeth hon, byddwn yn gweithio gyda llywodraethau datganoledig Cymru, yr Alban a Gogledd Iwerddon i sicrhau bod dull cyson yn cael ei fabwysiadu ar draws y wlad ar fentrau llywodraeth y DU ar faterion datganoledig, fel addysg a sgiliau. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

71. Cynnydd sylweddol yn nifer y bobl sydd â'r sgiliau sydd eu hangen arnynt i ymuno â'r gweithlu seiber, gan adeiladu ar y gwaith sy'n digwydd ar draws pedair gwlad y DU i sicrhau bod y polisi addysg a sgiliau yn diwallu gofynion pobl a chyflogwyr. Byddwn yn gwneud hyn drwy nifer o fesurau gan gynnwys ehangu rhaglenni hyfforddiant ôl-16 yn unol ag anghenion y gweithlu seiber, ariannu amrywiaeth o bwtcamps sgiliau ym maes seiberddiogelwch, cyflwyno rhaglen y Sefydliad Technoleg yn genedlaethol, a pharhau â chynllun bwrsarïau CyberFirst ar gyfer israddedigion. Mae hyn yn adeiladu ar waith y llywodraeth i gysoni'r rhan fwyaf o addysg a hyfforddiant ôl-16 â safonau cryfach sy'n cael eu harwain gan gyflogwyr erbyn 2030. Bydd y rhain yn cael eu datblygu ar y cyd â Chyngor Seiberddiogelwch y DU ar gyfer y gymuned seiber ehangach ac yn sail i brentisiaethau, Lefelau T a chymwysterau technegol uwch newydd. Bydd hyn yn sicrhau bod gan gyflogwyr rôl ganolog yn y gwaith o gynllunio a datblygu cymwysterau a hyfforddiant.

72. Proffesiwn seiberddiogelwch o ansawdd gwell sy'n gadarnach ac yn fwy cydnabyddedig a strwythuredig. Yn seiliedig ar Siarter Frenhinol, bydd Cyngor Seiberddiogelwch y DU yn sefydlu safonau proffesiynol a llwybrau i yrfa seiber a thrwy yrfa seiber, wedi'u hadeiladu ar y Corff Gwybodaeth Diogelwch Seiber (CyBOK) sydd gyda'r gorau yn y byd. A byddwn yn archwilio holl ddulliau ysgogi'r llywodraeth, gan gynnwys deddfwriaeth, er mwyn gwreiddio'r safonau hyn ar draws y proffesiwn, gan sicrhau bod rhagoriaeth ac arbenigedd yn gallu cael eu cydnabod yn glir ac yn gyson ar draws y gweithlu seiber.

73. Gweithlu seiber mwy amrywiol, gyda grwpiau sy'n cael eu tangynrychioli a'r rheini o gymunedau difreintiedig ledled y DU yn cael cymorth mwy effeithiol i ddechrau a ffynnu mewn gyrfa ym maes seiber. Bydd ein hystod o fesurau'n cynnwys cymorth i ragor o fenywod ymuno â'r gweithlu seiber ac ymyriadau penodol i gefnogi grwpiau sy'n cael eu tangynrychioli i symud ymlaen i lefelau uwch. A byddwn yn adeiladu ar lwyddiannau gweithgareddau allgyrsiol a gyflwynir drwy ein rhaglen CyberFirst flaenllaw, gan gynnwys Cystadleuaeth Merched CyberFirst. Byddwn hefyd yn cynyddu mynediad at addysg a chyfleoedd gyrfa i bobl ifanc sydd mewn perygl drwy raglen Cyber Choices yr Asiantaeth Troseddu Cenedlaethol, gan eu dargyfeirio oddi wrth weithgarwch seiber anghyfreithlon tuag at gyfleoedd mwy cadarnhaol i ddefnyddio eu doniau a'u brwdfrydedd.

74. Cyflenwad cyson ac amrywiol o bobl hyfedr yn dod drwy ein system addysg. Byddwn yn ysbrydoli ac yn cefnogi mwy o bobl ifanc i ddilyn llwybr technoleg drwy addysg, gan gynnwys cynnydd yn nifer yr ymgeiswyr sy'n dilyn TGAU Cyfrifiadureg a chymwysterau cyfatebol yn yr Alban, a mynd ymlaen i addysg bellach fel Lefelau T yn Lloegr a phrentisiaethau a chyfleoedd addysg uwch. Byddwn hefyd yn uwchsgilio mwy o athrawon yn Lloegr drwy'r Ganolfan Genedlaethol ar gyfer Addysg Cyfrifiadura (NCE), gan sicrhau eu bod yn gallu cael gafael ar yr adnoddau a'r cyfleoedd datblygu a fydd yn eu helpu i ysgogi diddordeb rhagor o fyfyrwyr.

75. Mae'r Llywodraeth mewn sefyllfa well i adnabod, i recriwtio, i hyfforddi ac i gadw'r gweithwyr seiber proffesiynol sydd eu hangen arni. Fel rhai sy'n cyflogi llawer o weithwyr seiber proffesiynol, bydd angen i'r llywodraeth a'r sector cyhoeddus arwain drwy esiampl, gan gefnogi ac adeiladu ar y mesurau a amlinellir uchod. Byddwn yn mabwysiadu dull gweithredu mwy cydlynol ac effeithiol ar draws y sector cyhoeddus, ar yr un pryd â theilwra mesurau penodol i wella sgiliau gweision sifil ac uwch arweinwyr, ac adeiladu ein gallu ym maes amddiffyn a diogelwch gan gynnwys yr NCF, yr NCSC ac asiantaethau gorfodi'r gyfraith. Bydd hyn yn cynnwys buddsoddi mewn doniau cynnar drwy ehangu'r Cyber Fast Stream a chynnig mwy o brentisiaethau seiberddiogelwch, cefnogi rhaglenni sgiliau arbenigol yn yr NCA gan gynnwys lleoliadau i raddedigion ac interniaid, rhaglenni niwroamrywiaeth pwrpasol a rhaglenni amrywiaeth yr haf. Bydd yn adeiladu ar lwyddiannau'r Ysgol Seiber Amddiffyn drwy ei hymestyn i'r Academi Seiber Amddiffyn gyda chynnig ehangach o hyfforddiant seiber amddiffynnol ac ymosodol, tra'n cydweithio â phartneriaid academaidd, diwydiant a rhyngwladol.

Cyngor Seiberddiogelwch y DU

Cafodd Cyngor Seiberddiogelwch y DU ei lansio ym mis Mawrth 2021 a dyma'r cyntaf yn y byd ar gyfer y proffesiwn seiberddiogelwch. Ei genhadaeth yw bod yn llais i'r proffesiwn, gan ddod ag eglurder a strwythur i'r gweithlu seiber sy'n tyfu a'r ystod o gymwysterau, ardystiadau a graddau sy'n bodoli ar draws y maes. Mae hwn yn gam hollbwysig, gan gydnabod bod y proffesiwn seiber yn cynnwys amrywiaeth eang o arbenigeddau ac arbenigaethau technegol ac annhechnegol ar draws yr economi, sy'n debyg o ran ehangder i broffesiynau mwy sefydledig fel meddygaeth a'r gyfraith.

Mae gan y Cyngor bedwar nod:

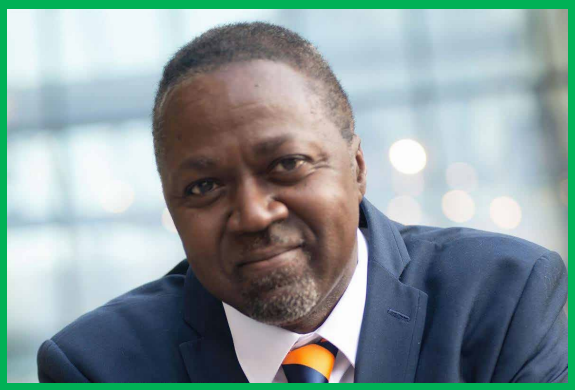
- Arwain agweddau a safonau proffesiynol: arwain y gwaith i ddatblygu a chytuno ar y safonau sy'n diffinio seiberddiogelwch
- Gyrfaoedd a dysgu: cefnogi cyflogwyr ac unigolion wrth iddynt wneud penderfyniadau am yrfaoedd, gyda chyngor ar sgiliau seiberddiogelwch, datblygiad proffesiynol a chydnabyddiaeth
- Moeseg broffesiynol: darparu egwyddorion arweiniol lle gall gweithwyr proffesiynol sy'n gweithio yn y maes a sefydliadau eu hunain ddangos arferion moesegol mewn seiberddiogelwch
- Amrywiaeth a chynhwysiant: hyrwyddo seiberddiogelwch fel cyfle gyrfa i bobl o bob oed a chefndir, gan ymdrechu i chwalu rhwystrau rhag mynediad a dilyniant yn y maes

Bydd y Cyngor yn ceisio tyfu a sefydlu ei hygrededd a'i gynaliadwyedd fel yr awdurdod proffesiynol gydol oes y strategaeth hon. Bydd yn dwyn ynghyd amrywiaeth o gyrff proffesiynol ac ardystio sy'n bodoli eisoes, gan nodi a grymuso sefydliadau arbenigol sy'n gallu darparu eglurder ynghylch gofynion dilyniant a chymhwysedd i newydd-ddyfodiaid, ymarferwyr presennol a chyflogwyr fel ei gilydd.

Cymeradwyodd y Frenhines ddyfarnu Siarter Frenhinol i Gyngor Seiberddiogelwch y DU ym mis Tachwedd 2021. Am y tro cyntaf, mae hyn yn darparu cydnabyddiaeth siartredig bwrpasol yn benodol ar gyfer seiberddiogelwch, sy'n cwmpasu'r ystod o arbenigeddau sy'n bodoli yn y maes.

Rydym yn cydnabod bod mwy o waith i'w wneud i wreiddio safonau a llwybrau proffesiynol ar draws yr ecosystem seiber, gan gynnwys ar draws y llywodraeth, amddiffyn ac asiantaethau gorfodi'r gyfraith. Bydd y Cyngor yn chwarae rhan bwysig yn hyn, gan gefnogi pobl ifanc a phobl sy'n newid gyrfa i lywio eu gyrfa ym maes seiber.

Simon Hepburn, Prif Swyddog Gweithredol, Cyngor Seiberddiogelwch y DU



Mae fy ngwaith yn cynnwys hyrwyddo Cyngor Seiberddiogelwch y DU fel "llais y proffesiwn seiberddiogelwch." Y Cyngor yw'r corff hunanreoleiddiol ar gyfer proffesiwn seiberddiogelwch y DU, a'n nod yw uno'r diwydiant i ddatblygu, hyrwyddo a gwarchod safonau sy'n cael eu cydnabod yn genedlaethol ar gyfer seiber er mwyn gwneud y DU y lle mwyaf diogel i fyw a gweithio ar-lein. Cafodd y Cyngor ei lansio'n swyddogol ym mis Mawrth 2021 yn dilyn prosiect ffurfio llwyddiannus, ac rydym nawr yn derbyn ceisiadau am aelodaeth. Mae'r Strategaeth Seiber Genedlaethol yn elfen hanfodol i sicrhau bod unigolion a sefydliadau yn gallu gweithio mewn modd sy'n hyrwyddo'r proffesiwn, gyda'r Cyngor yn chwaraewr cydlynu allweddol.

Amcan 3: Meithrin twf sector seiberddiogelwch a diogelwch gwybodaeth cynaliadwy, arloesol a chystadleuol yn rhyngwladol, gan ddarparu cynnyrch a gwasanaethau o safon, sy'n diwallu anghenion y llywodraeth a'r economi ehangach

76. Er mwyn gwella ein pŵer seiber cenedlaethol a sbarduno twf ac allforion digidol, mae angen i'r DU gael sector seiber bywiog sy'n cynnwys cwmnïau o ansawdd uchel y gellir ymddiried ynddynt. Mae cwmnïau yn y DU yn darparu technolegau, hyfforddiant a chyngor o'r radd flaenaf i ddiwydiant a llywodraethau yn y DU ac yn fyd-eang. Ond i ddatblygu technolegau arloesol, mae rhai cwmnïau angen cefnogaeth a chysylltiadau i fuddsoddi er mwyn cyrraedd y cam lle gallant gynnig cynnyrch ymarferol.

77. Mae angen i gwmnïau hefyd deimlo'n hyderus eu bod yn arloesi yn unol â pharamedrau cymeradwy'r llywodraeth y mae sefydliadau eraill hefyd yn eu dilyn. Ac mae mwy y gallwn ni ei wneud i helpu prynwyr i lywio drwy'r dirwedd gymhleth, gydag amrywiaeth enfawr o gynnyrch a gwasanaethau o ansawdd amrywiol. Bydd hyn, yn ei dro, yn ysgogi'r galw yn yr ecosystem ac yn cefnogi twf pellach. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

78. Sector seiber sydd wedi cyflawni mwy na'r cyfartaledd o dwf byd-eang o un flwyddyn i'r llall, gan gynnwys drwy fasnach ac allforion seiber. Byddwn yn helpu busnesau seiber i gael mynediad at farchnadoedd newydd gartref a thramor drwy gefnogi digwyddiadau seiber blaenllaw sydd gyda'r gorau yn y byd yma yn y DU a gwahodd ein busnesau seiber mwyaf arloesol i gymryd rhan mewn teithiau masnach a ffeiriau seiber rhyngwladol. A byddwn yn defnyddio caffael yn y sector cyhoeddus yn fwy effeithiol ac yn sefydlu cyfeiriadur cynhwysfawr o ddarparwyr achrededig NCSC i hybu'r galw am gynnyrch a gwasanaethau seiberddiogelwch o ansawdd uchel.

79. Sector seiber hyd yn oed mwy arloesol sydd wedi gweld cynnydd sylweddol mewn buddsoddiad yn y cyfnod cynnar a mwy o fusnesau seiber sydd wedi gallu lansio, tyfu a datblygu. Mae ein rhaglen newydd, Cyber Runway, yn rhoi un pwynt cyswllt i fusnesau ar gyfer cymorth, gan ddysgu gwersi o'n rhaglenni blaenorol fel Rhaglen Seiber Tech Nation, Cyber101 a Hut Zero. Byddwn yn trawsnewid Canolfan Arloesi Cheltenham, sy'n cynnwys y cyflymydd seiber 'NCSC for Startups', yn ganolfan arloesi ryngwladol go iawn: y Ganolfan Arloesi Seiber Genedlaethol. Byddwn yn defnyddio arbenigedd sefydliadau sy'n bodoli i hyrwyddo ac i alluogi cyd-greu, fel y Gyfnewidfa Technoleg ac Arloesi Diogelwch Cenedlaethol. A byddwn yn annog buddsoddiad risg uwch mewn busnesau seiber newydd, gan gynnwys drwy'r Gronfa Buddsoddi Strategol mewn Diogelwch Gwladol, mewn partneriaeth â Banc Busnes Prydain

80. Economi seiber yn y DU sydd wedi cael ei chysoni'n sylweddol gyda thwf cynyddol y tu allan i'r De Ddwyrain, gan gyfrannu at adferiad o bandemig y coronafeirws (COVID-19) a chefnogi gweithgarwch economaidd rhanbarthol ehangach. Byddwn yn sefydlu pencadlys parhaol NCF yn Samlesbury, yng Ngogledd Orllewin Lloegr, gan sbarduno twf yn y sectorau technoleg, digidol ac amddiffyn y tu allan i Lundain a helpu i greu partneriaethau newydd yn y rhanbarth. Byddwn yn cynyddu ein cefnogaeth i arloeswyr ac entrepreneuriaid y tu allan i Lundain a De Ddwyrain Lloegr i ddatblygu eu cynnyrch a'u gwasanaethau, i dyfu eu busnesau ac i recriwtio staff medrus. Mae hyn yn cynnwys campws Golden Valley dan arweiniad Cyngor Bwrdeistref Cheltenham sydd wedi ymrwymo i gefnogi twf busnesau technoleg sy'n gysylltiedig â seiberddiogelwch. A byddwn yn cynyddu gallu allforio cwmnïau seiber ar draws mwy o ranbarthau'r DU drwy ymgysylltu â'r clystyrau seiber rhanbarthol a digwyddiadau penodol i arddangos mwy o'n doniau yn y diwydiant seiber i brynwyr rhyngwladol.

81. Mae mwy o gwmnïau'n gallu cynnig technolegau, cynnyrch a gwasanaethau seiberddiogelwch sy'n cyrraedd safonau ansawdd sydd wedi'u dilysu'n annibynnol, gan godi hyder defnyddwyr. Byddwn yn cyflawni hyn yn unol â'r papur gwyn Dyfodol NCSC ar Sicrhau Technoleg a gyhoeddwyd gan y NCSC ym mis Medi 2021, gan ddefnyddio brand ac arbenigedd NCSC i greu marchnad y gellir ymddiried ynddi a fydd yn helpu defnyddwyr yn y DU i brynu gwasanaethau'n hyderus, gwella eu diogelwch a chodi'r bar yn genedlaethol o ran seiberddiogelwch.[23]

[23] NCSC, White paper: The future of NCSC Technology Assurance (2021)

Berta Pappenheim, Prif Swyddog Gweithredol a sylfaenydd, Cyberfish Company

Cymerodd CyberFish ran mewn rhaglen cyflymydd seiber gan y llywodraeth. Ein nod yw helpu busnesau a thimau'r llywodraeth i baratoi i ddelio'n well â digwyddiadau sy'n amharu ar fusnes, fel digwyddiadau seiber. Rydym yn gwneud hyn drwy gynnal ymarferion efelychu digwyddiadau gyda nhw, arsylwi deinameg eu tîm o dan straen, a'u hyfforddi ar sut i wneud gwelliannau. Mae llawer o gynghorwyr yn dda am naill ai'r ochr dechnegol i ymateb i ddigwyddiadau, neu ochr ymddygiadol arweinyddiaeth a gwneud penderfyniadau. Rydyn ni'n gwneud y naill a'r llall, gyda'i gilydd, gyda gwybodaeth arbenigol o'r naill ochr a'r llall. Mae ein hymarferion wedi helpu bron i 500 o arweinwyr y diwydiant sy'n gweithio mewn timau hanfodol ar draws y byd i newid safbwyntiau, gwella eu gwaith tîm, gan arwain at ymateb yn well i argyfyngau a gwneud penderfyniadau gwell.

Oes gennych chi awydd ymuno â'r gweithlu seiber neu gychwyn eich busnes eich hun?

82. Roedd ein strategaeth flaenorol yn rhoi pwyslais mawr ar dyfu'r sylfaen sgiliau seiber a'r sector gwasanaethau seiberddiogelwch yn y DU. Fel yr amlinellwyd yn y cyd-destun strategol, rydym wedi gwneud cynnydd sylweddol o ran **tyfu'r sector ac allforion**:

Helpu busnesau seiber i ddod o hyd i farchnadoedd rhyngwladol. Roedd y DU wedi allforio £4.2 biliwn o wasanaethau seiber yn 2020.

Cyber Exchange, ein porth seiber ar-lein, sy'n dod â busnesau seiber at ei gilydd o bob rhanbarth yn y DU.

Mae'r Bartneriaeth Twf Seiber wedi bod yn dod â llywodraeth a diwydiant at ei gilydd i chwalu'r rhwystrau sy'n atal twf.

83. Rydyn ni wedi **cefnogi arloeswyr i dyfu eu busnesau**, gan sicrhau bod ecosystem seiber y DU wedi ffynnu dros y pum mlynedd diwethaf:

NCSC for Startups sy'n cyfeirio arloeswyr at yr heriau strategol pwysicaf ac mae ei fusnesau a'i gwmnïau wedi cymryd rhan mewn dros 160 o dreialon corfforaethol newydd yn barod.

LORCA sydd wedi helpu 72 o arloeswyr seiber i godi dros £200 miliwn o fuddsoddiad ac ennill dros £37 miliwn o refeniw.

Cyber Runway sy'n cefnogi arloeswyr i lansio ac i dyfu eu busnes – gan adeiladu ar lwyddiant Hutzero a Cyber101.

84. Rydyn ni wedi bod yn gweithio i leihau'r diffyg blynyddol o 10,000 o weithwyr proffesiynol sy'n **ymuno â'r gweithlu seiber**:[24]

Cynllun bwrsari CyberFirst sy'n cefnogi myfyrwyr israddedig ac mae'n cynnig profiad gwaith i gannoedd o unigolion yn y gweithlu seiber bob blwyddyn.

Mae pedair safon ar gyfer prentisiaethau seiber erbyn hyn sydd wedi cael eu dylunio gan y diwydiant a thri chynnig seiber ar gyfer canlyniadau dysgu cychwynnol a gynigir drwy fenter 'Courses for Jobs' yr Adran Addysg.

Cynhaliwyd naw bwtcamp seiber gyda chefnogaeth y Gronfa Sgiliau Genedlaethol ddiweddar, a oedd yn arwain pobl i yrfaoedd seiber cyffrous ac mae mwy o'r rhain ar y gweill ar gyfer pob blwyddyn o'r cyfnod gwario nesaf.

85. Rydym wedi bod yn **proffesiynoli'r gweithlu seiber**, sy'n golygu ei bod hi'n symlach i sefydliadau ddeall pa sgiliau sydd eu hangen arnynt, a'i gwneud hi'n haws i unigolion lywio drwy'r hyn y mae angen iddynt ei wybod:

Cyngor Seiberddiogelwch y DU sy'n awdurdod proffesiynol cyntaf yn y byd ar gyfer seiberddiogelwch. Mae wedi dechrau gosod safonau proffesiynol clir a chyson, gan adeiladu ar yr holl waith y mae'r cyrff proffesiynol presennol wedi'i wneud hyd yma. Bydd y Cyngor yn ceisio nodi'n glir gymwysterau effeithiol o'r llu sydd ar gael ar hyn o bryd.

Mae Corff Gwybodaeth Diogelwch Seiber (CyBOK) yn rhoi gwybodaeth a sylfaen ar gyfer addysg a hyfforddiant proffesiynol i'r sector seiberddiogelwch.

[24] Yr Adran dros Dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon, Understanding the cyber security recruitment pool (2021)

86. Rydym wedi bod yn gweithio i **sicrhau bod pawb yn gallu ymuno â'r gweithlu seiber**, gan fynd i'r afael ag anghydraddoldeb yn y sector lle mai dim ond 16% o'r gweithlu sy'n fenywod, a dim ond 3% o'r uwch swyddi sy'n cael eu dal gan fenywod a lleiafrifoedd ethnig.[25]

Mae'r cyrsiau CyberFirst a'r rhaglen Discovery wedi ymgysylltu â bron i 300,000 o bobl ifanc 11-17 oed yn ystod y pum mlynedd diwethaf.

Mae'r UK Cyber Cluster Collaboration yn llunio partneriaethau rhwng diwydiant, ysgolion a cholegau i sicrhau bod cyfleoedd ac arbenigedd ar gael ar draws y rhanbarthau.

Mae rhaglen Cyber Choices yr NCA yn helpu pobl ifanc i wneud dewisiadau gwybodus a defnyddio eu sgiliau seiber mewn ffordd gyfreithiol, gan godi ymwybyddiaeth a darparu dewisiadau amgen fel prentisiaethau a lleoliadau gwaith

[25] Llywodraeth Ei Mawrhydi, Cyber security skillls in the UK labour market (2021)

Colofn 2:
Seibergadernid

Adeiladu DU ddigidol gadarn a ffyniannus

87. Mae seiberddiogelwch a seibergadernid yn sylfaenol i'n nodau strategol ehangach fel pŵer seiber: hebddynt, ni allwn obeithio manteisio i'r eithaf ar botensial trawsnewidiol technolegau digidol i adeiladu'n ôl yn well, yn decach ac yn gryfach, ac i ddiogelu mantais strategol y DU mewn seiberofod a drwyddo. Rhaid i ni barhau i feithrin amddiffyniadau seiber cryf, gan gymryd camau i ddiogelu rhwydweithiau digidol, gwybodaeth ac asedau'r DU ar lefel genedlaethol, leol ac unigol a sicrhau eu bod yn gadarn pan fydd digwyddiadau'n codi.

88. Ac er ein bod yn canolbwyntio yn y bennod hon ar seibergadernid, er mwyn bod yn gwbl effeithiol, bydd angen i hyn fod yn rhan o ymdrech gyfannol a chymdeithas gyfan i wella cadernid y DU. Bydd y Strategaeth Cadernid Genedlaethol sydd ar y gweill, un o brif ymrwymiadau'r Adolygiad Integredig, yn nodi'r dull gweithredu cyffredinol ar gyfer cadernid cenedlaethol.

89. Mae cynnydd sylweddol wedi cael ei wneud yn ystod y degawd diwethaf o ran gwella ein gwytnwch seiber, gyda sefydlu'r Ganolfan Seiberddiogelwch Genedlaethol (NCSC), mae mwy o gyngor, arweiniad ac adnoddau eraill ar gael, a gweithredu deddfwriaeth gan gynnwys Rheoliadau Rhwydweithiau a Systemau Gwybodaeth (Rheoliadau NIS), y Rheoliad Diogelu Data Cyffredinol a Deddf Diogelu Data 2018. Ond mae bylchau difrifol yn dal i fodoli. Mae achosion o dorri diogelwch seiber yn effeithio ar y llywodraeth, busnesau, sefydliadau ac unigolion; mae llawer o sefydliadau'n dal i roi gwybod am nifer fawr o ymosodiadau neu achosion o dorri diogelwch seiber.

90. Rydym yn adeiladu ar sylfeini'r strategaeth flaenorol, yn esblygu ein dull gweithredu ac yn symud yn gyflymach ar seibergadernid y DU – gan roi pwyslais penodol ar y canlynol:

- cynyddu ein gwaith i wneud y rhyngrwyd yn fwy diogel yn awtomatig, atal ymosodiadau, cynnwys mesurau diogelu sylfaenol er budd holl fusnesau, sefydliadau a dinasyddion y DU, a chynyddu'r cymorth sydd ar gael i'r rheini sydd leiaf abl i amddiffyn eu hunain ar-lein
- gosod uchelgais i'r llywodraeth weithredu fel esiampl o arfer gorau ym maes seiberddiogelwch
- gwreiddio seiberddiogelwch fel rhan greiddiol o fusnes da drwy ddefnyddio rheoleiddio a chymhellion eraill yn well, a harneisio pŵer ein dealltwriaeth o fygythiadau i adeiladu cymunedau sy'n gallu amddiffyn eu hunain
- ategu hyn i gyd gyda safonau gwrthrychol, tystiolaeth a data a symud o gasglu i weithredu ar y data hwnnw

91. Yn y strategaeth hon, mae tair agwedd allweddol i'r cysyniad o seibergadernid. Yn gyntaf, mae angen deall natur y **risg**. Yn ail, mae angen gweithredu i **sicrhau** systemau i atal a gwrthsefyll ymosodiadau seiber. Yn drydydd, gan gydnabod y bydd rhai ymosodiadau'n dal i ddigwydd, mae angen i ni baratoi ar gyfer y rhain, bod yn ddigon **cadarn** i leihau eu heffaith a gallu adfer.

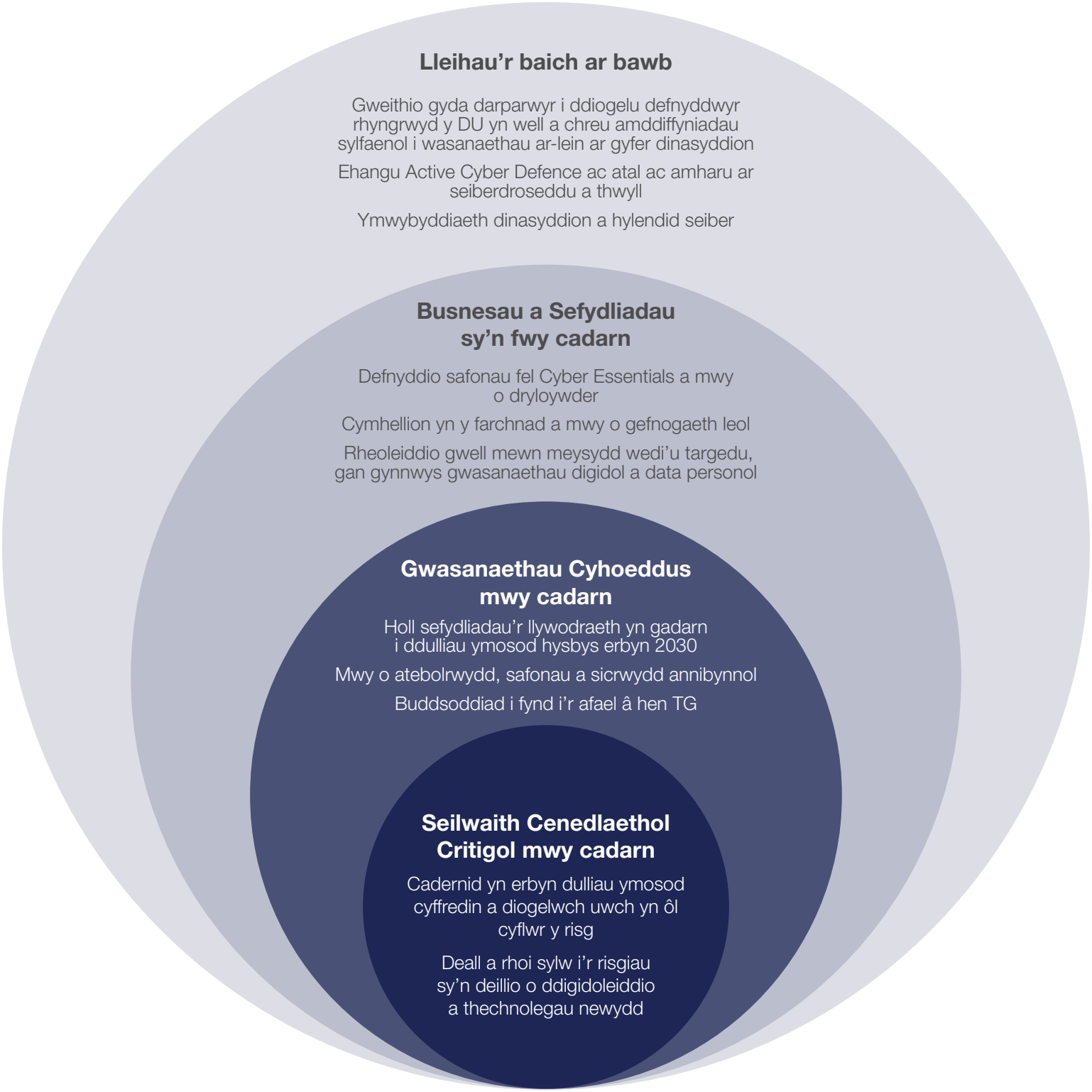
92. Bydd ein dull yn cael ei deilwra ar gyfer pob cynulleidfa, wedi'i gefnogi gan alluoedd cenedlaethol sy'n ein galluogi i fynd i'r afael â risgiau systemig. Y cynulleidfaoedd rydym yn ceisio eu diogelu a dylanwadu arnynt yw dinasyddion, busnesau a sefydliadau'r DU, y llywodraeth a'r sector cyhoeddus, a'r rheini sy'n gweithredu ein seilwaith cenedlaethol hanfodol (gan ddarparu'r gwasanaethau allweddol fel dŵr yfed, trydan, cyllid, trafnidiaeth a thelathrebu - pethau rydym i gyd yn dibynnu arnynt).

93. Byddwn yn canolbwyntio'n gyntaf ar gamau i ddiogelu'r amgylchedd digidol ar gyfer pawb yn y DU sy'n defnyddio'r rhyngrwyd, atal ymosodiadau, adeiladu diogelwch sylfaenol mewn cynnyrch a gwasanaethau, a helpu unigolion a busnesau bach a sefydliadau gyda chamau gweithredu sylfaenol i wella seiberddiogelwch. Wrth i ni symud ymlaen at y rheini sydd â mwy o gyfrifoldeb a gallu i sefydlu haenau ychwanegol o ddiogelwch a chadernid sy'n gymesur i'r risg, bydd hyn yn arwain at y lefel uchaf o ddiogelwch a ddisgwylir ar gyfer y gwasanaethau cyhoeddus a hanfodol allweddol y mae ein pobl a'n heconomi yn dibynnu arnynt.

94. Rhaid i hyn fod yn ymdrech ar y cyd rhwng y llywodraeth a phob rhan o'r economi a chymdeithas. Cyfrifoldeb byrddau busnesau a sefydliadau yw rheoli eu risg seiber eu hunain. Ein nod yw gosod disgwyliadau clir wedi'u hategu gan y fframwaith cywir o gymhellion, cymorth a rheoleiddio i alluogi gwelliannau a throsglwyddo baich risg seiberddiogelwch oddi wrth ddefnyddwyr a thuag at y rhai sydd yn y sefyllfa orau i'w rheoli.

95. Rydym yn mynnu bod adrannau'r llywodraeth, y sector cyhoeddus ehangach a gweithredwyr seilwaith cenedlaethol hanfodol sy'n cael eu rheoleiddio (CNI), yn codi eu safonau ac yn rheoli eu risg yn fwy rhagweithiol. Rydym yn disgwyl i fusnesau a sefydliadau mawr, gan gynnwys darparwyr gwasanaethau a phlatfformau digidol, fod yn fwy atebol am ddiogelu eu systemau, eu gwasanaethau a'u cwsmeriaid fel rhan greiddiol o redeg eu busnes. Yn gyfnewid am hynny, bydd y llywodraeth yn gwneud mwy i ddiogelu'r amgylchedd digidol a mynd i'r afael â risgiau systemig a darparu cymorth drwy gyngor, offer, achrediad yn y farchnad, a datblygu'r sgiliau sy'n galluogi gwelliannau.

96. Rhaid i'n hymdrechion i hyrwyddo seibergadernid yn y DU hefyd fod yn rhan o'n hymgysylltiad rhyngwladol. Mae globaleiddio cynyddol cadwyni cyflenwi, platfformau TG, busnesau rhyngwladol, a'r rhyngrwyd ei hun, yn golygu na allwn wella seiberddiogelwch y DU ar ei ben ei hun. Er mwyn ymateb i'r her hon, bydd angen i ni barhau i feithrin gwell dealltwriaeth o'r cysylltiadau rhwng seibergadernid y DU a'r byd, gan fynd i'r afael â meysydd risg uchel a gweithio gyda phartneriaid rhyngwladol i feithrin gwytnwch sy'n hwyluso trawsnewid digidol, diogelwch a masnach, er budd y naill a'r llall fel y nodir yng Ngholofn 4: Pennod Arweinyddiaeth Fyd-eang.


Lleihau'r baich ar bawb
Gweithio gyda darparwyr i ddiogelu defnyddwyr rhyngrwyd y DU yn well a chreu amddiffyniadau sylfaenol i wasanaethau ar-lein ar gyfer dinasyddion
Ehangu Active Cyber Defence ac atal ac amharu ar seiberdroseddu a thwyll
Ymwybyddiaeth dinasyddion a hylendid seiber
Busnesau a Sefydliadau sy'n fwy cadarn
Defnyddio safonau fel Cyber Essentials a mwy o dryloywder
Cymhellion yn y farchnad a mwy o gefnogaeth leol
Rheoleiddio gwell mewn meysydd wedi'u targedu, gan gynnwys gwasanaethau digidol a data personol
Gwasanaethau Cyhoeddus mwy cadarn
Holl sefydliadau'r llywodraeth yn gadarn i ddulliau ymosod hysbys erbyn 2030
Mwy o atebolrwydd, safonau a sicrwydd annibynnol
Buddsoddiad i fynd i'r afael â hen TG
Seilwaith Cenedlaethol Critigol mwy cadarn
Cadernid yn erbyn dulliau ymosod cyffredin a diogelwch uwch yn ôl cyflwr y risg
Deall a rhoi sylw i'r risgiau sy'n deillio o ddigidoleiddio a thechnolegau newydd

Amcan 1: Gwella dealltwriaeth o risg seiber er mwyn sbarduno gweithredu mwy effeithiol ar seiberddiogelwch a seibergadernid

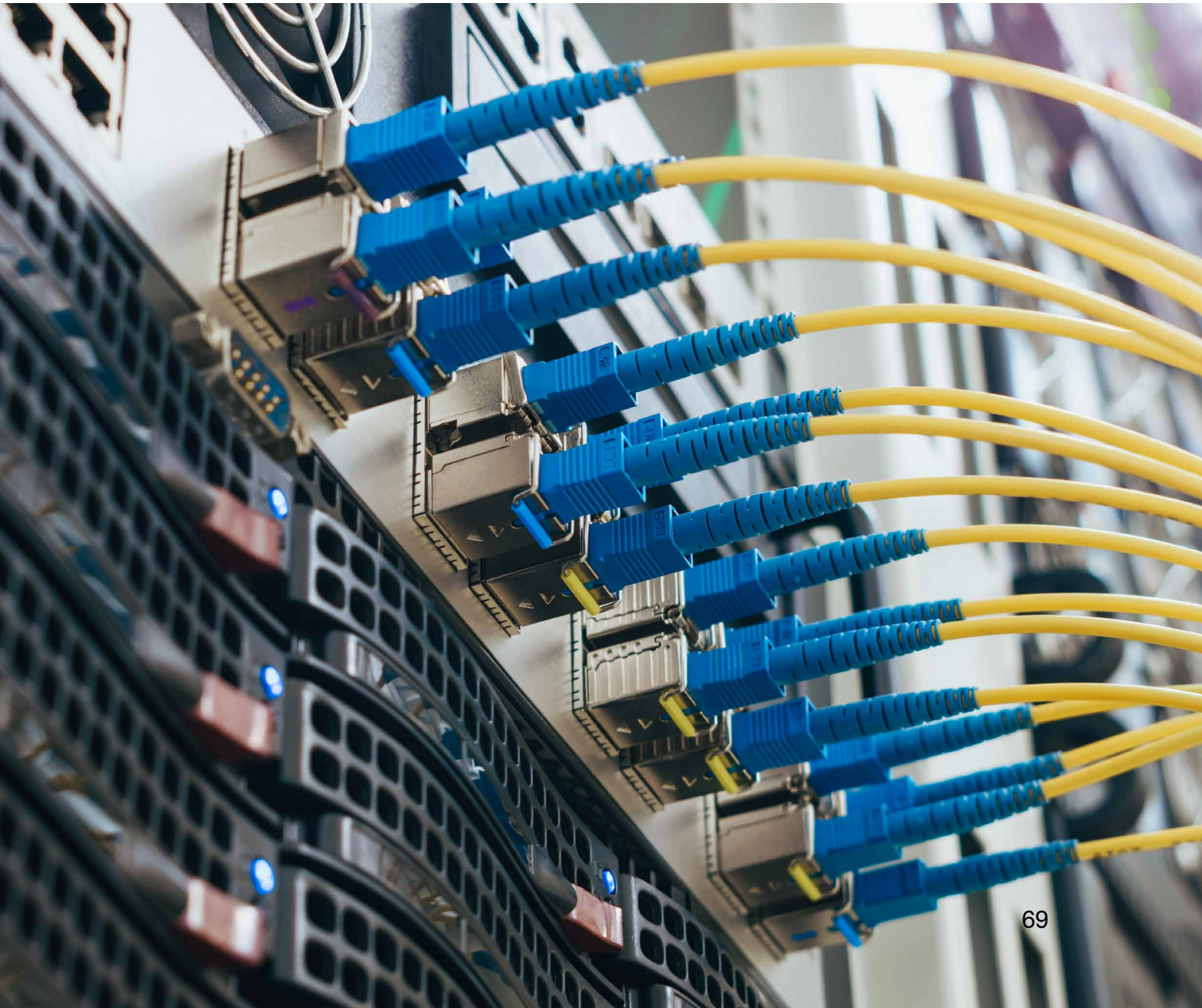
97. Byddwn yn darparu partneriaeth llawer agosach rhwng y llywodraeth, busnesau a sefydliadau er mwyn gwella cyd-ddealltwriaeth o'r risg, llywio'r gwaith blaenoriaethu a sefydlu'r achos dros weithredu. Byddwn yn cefnogi dinasyddion drwy weithio gyda busnesau a sefydliadau sy'n darparu gwasanaethau i ddefnyddwyr; ac yn cryfhau gallu'r llywodraeth i adnabod risgiau trawsbynciol ymhellach. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

98. Mae gan y Llywodraeth ddealltwriaeth strategol gyfredol o seiberddiogelwch y wlad ac mae'n defnyddio'r ddealltwriaeth hon i nodi risgiau systemig, i gyfleu blaenoriaethau ac i sbarduno strategaeth a chyflawni. Byddwn yn cynnal ac yn ysgogi rhagor o werth o fuddsoddiadau sylweddol a wneir mewn 'deall y bygythiad' o'r Strategaeth Seiberddiogelwch Genedlaethol flaenorol; ac yn adeiladu ar yr ymdrechion presennol i ddeall risg mewn byd sy'n dod yn fwyfwy rhyng-gysylltiedig. Bydd hyn yn cynnwys nodi lle mae cadwyni cyflenwi digidol wedi'u crynhoi'n ormodol, a gweithio gyda phartneriaid rhyngwladol i reoli risgiau ar y cyd. Byddwn hefyd yn gwella sut rydym yn cofnodi troseddau Deddf Camddefnyddio Cyfrifiaduron (CMA), gan ddeall y cysylltiadau rhwng torri diogelwch data a throseddau sy'n deillio o hynny, a chynyddu ein gwybodaeth am sut mae troseddau CMA yn hwyluso mathau eraill o weithgarwch troseddol.

99. Mae'r Llywodraeth yn arwain drwy esiampl yn ei dealltwriaeth o risg seiber. Byddwn yn mabwysiadu Fframwaith Asesu Seiber yr NCSC fel y fframwaith sicrwydd ar gyfer holl adrannau'r llywodraeth, a bydd systemau critigol a chyflenwyr cyffredin yn cael eu mapio. Byddwn yn sefydlu Canolfan Cydgysylltu Seiber newydd y Llywodraeth (GCCC) a Gwasanaeth Adrodd ar Wendidau (VRS) ar draws y Llywodraeth er mwyn galluogi'r llywodraeth i 'amddiffyn fel un' wrth reoli digwyddiadau, gwendidau a bygythiadau. Bydd y VRS yn ceisio meithrin cysylltiadau gwerthfawr a dibynadwy gyda'r gymuned ymchwilwyr diogelwch, gan arwain at ostyngiad mewn gwendidau ar draws ystad y llywodraeth. Byddwn hefyd yn parhau i gefnogi a chydlynu cynlluniau tebyg yn y llywodraethau datganoledig, fel y bwriad i sefydlu swyddogaeth gydlynu ganolog ar gyfer seibergadernid yn yr Alban.

100. Ar draws CNI y DU, bydd gennym ddealltwriaeth fwy soffistigedig o risgiau seiber. Byddwn yn cynyddu faint sy'n mabwysiadu'r Fframwaith Asesu Seiber (CAF) neu gyfatebol ar draws sectorau CNI, ac yn gwella'r gallu i gymharu â fframweithiau adrodd ac asesu seiberddiogelwch eraill sy'n cael eu defnyddio. Byddwn yn cwblhau adolygiadau critigoldeb ac yn mapio dibyniaethau o fewn CNI a'i gadwyni cyflenwi. Byddwn yn adeiladu partneriaethau cryfach gyda pherchnogion a gweithredwyr CNI i wella mynediad at wybodaeth am fygythiadau a risg, a chytuno ar gyflwr risgiau. A byddwn yn gweithio i ddeall risgiau newydd neu lle mae CNI newydd yn dod i'r amlwg o ganlyniad i ddigideiddio a thechnolegau newydd, gan gynnwys fel rhan o flaenoriaethau ehangach fel y trawsnewid i Sero Net.

101. Mae gan fusnesau a sefydliadau yn y DU well dealltwriaeth o risgiau seiber a'u cyfrifoldebau i'w rheoli. Byddwn yn helpu sefydliadau i ddeall y risg i'w cwsmeriaid yn well, gan gynnwys sut gellid defnyddio'r data sydd ganddynt i hwyluso troseddau fel twyll, dwyn hunaniaeth neu orfodaeth. A byddwn yn rhannu mwy o wybodaeth o ymchwil a data am ba mor gyffredin yw ymosodiadau seiber a'r cynnydd cymharol y mae sectorau yn ei wneud o ran gwella seiberddiogelwch.



Amcan 2: Atal a gwrthsefyll ymosodiadau seiber yn fwy effeithiol drwy wella'r gwaith o reoli risg seiber yn sefydliadau'r DU, a darparu mwy o amddiffyniad i ddinasyddion

102. Mae ein dull o atal a gwrthsefyll ymosodiadau seiber yn tybio: (i) bod gan sefydliadau gyfrifoldeb i gymryd camau i reoli eu risgiau seiber eu hunain ond mae angen fframweithiau atebolrwydd a llywodraethu da cryfach ar lefel bwrdd i wneud hyn yn flaenoriaeth; (ii) bod rôl i'r llywodraeth weithio gyda'r diwydiant i gymryd camau i leihau risg yn uniongyrchol ar raddfa lle mae mewn sefyllfa unigryw i wneud hynny; a (iii) rhaid i ni sicrhau bod cymorth ac arweiniad ar gael i helpu unigolion, masnachwyr unigol a busnesau bach a sefydliadau i reoli eu risgiau seiber. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

103. Mae'r Llywodraeth wedi lleihau niwed i'r DU ar raddfa fawr ac wedi lleihau'r baich ar ddinasyddion y DU. Byddwn yn gweithredu fwyfwy ar lefel uwch ar ran holl ddefnyddwyr y rhyngrwyd yn y DU, gan ehangu ein mesurau Active Cyber Defence i gefnogi ystod ehangach o sectorau, gan gynnwys elusennau, y byd academaidd, dinasyddion a busnesau bach a chanolig eu maint. A byddwn yn cryfhau'r amddiffyniadau i wasanaethau ar-lein drwy ymgysylltu'n well a rhannu gwybodaeth â'r diwydiant.

104. Mae'r gwaith hwn yn cyd-fynd â blaenoriaethau eraill y llywodraeth sydd wedi'u hanelu at ddiogelu dinasyddion y DU ar-lein, fel y Bil Diogelwch Ar-lein drafft a pholisi i wrthsefyll troseddau economaidd fel twyll.

105. Bydd yn golygu gweithio'n agosach gyda sectorau perthnasol gan gynnwys darparwyr gwasanaethau ar-lein, telegyfathrebu, technoleg, bancio ac adwerthu, i ddiogelu defnyddwyr rhyngrwyd y DU yn well, gan gynnwys: ei gwneud hi'n anoddach cofrestru gwefannau at ddibenion anghyfreithlon, rhwystro a dileu mwy o gynnwys maleisus ar-lein, gwella'r broses o adfer a dychwelyd manylion adnabod sydd wedi'u dwyn, a gwella diogelwch seilwaith telathrebu'r DU. Byddwn hefyd yn datblygu opsiynau i roi cefnogaeth statudol i warchod dinasyddion os bydd trefniadau gwirfoddol yn annigonol.

106. Bydd ein hymdrechion i leihau niwed ar raddfa fawr hefyd yn cynnwys mynd i'r afael â risgiau systemig o'r gadwyn gyflenwi ddigidol. Lle bo angen, byddwn yn ymyrryd i hyrwyddo arallgyfeirio yn y gadwyn gyflenwi, fel rydym yn ei wneud mewn telathrebu; byddwn yn cryfhau ein diogelwch economaidd ar y cyd drwy rannu gwybodaeth yn well a defnyddio dulliau cadarn, rhagweladwy a chymesur i sgrinio buddsoddiadau uniongyrchol o dramor (FDI) mewn sectorau allweddol, ac yn sefydlu gofynion clir ar gyfer cyflenwyr allweddol a chyffredin i'r llywodraeth.

107. Mae swyddogaethau hanfodol llywodraeth yn fwy cadarn o lawer i wrthsefyll ymosodiadau seiber a bydd holl sefydliadau'r llywodraeth – ar draws y sector cyhoeddus – yn gallu gwrthsefyll gwendidau a dulliau ymosod hysbys erbyn 2030. Ein nod yw sefydlu sector cyhoeddus y DU fel enghraifft o arfer gorau. I gefnogi'r canlyniad hwn, byddwn yn cyhoeddi Strategaeth Seiberddiogelwch bwrpasol gyntaf y Llywodraeth. Bydd hyn yn canolbwyntio ar brosesau rheoli risg, llywodraethu ac atebolrwydd mwy effeithiol; galluoedd sy'n cael eu datblygu a'u defnyddio'n ganolog (gan gynnwys Active Cyber Defence); monitro systemau, rhwydweithiau a gwasanaethau yn fwy cynhwysfawr; ymateb cyflym ac ar raddfa i ddigwyddiadau; a buddsoddi mewn sgiliau, gwybodaeth a diwylliant sy'n hyrwyddo newid cynaliadwy.

108. Mae risgiau seiber i seilwaith cenedlaethol hanfodol yn y DU yn cael eu rheoli'n fwy effeithiol. Gwasanaethau o'r fath yw'r rhai y mae'r wlad yn dibynnu arnynt fwyaf. Byddwn yn parhau i weithio'n agos gyda gweithredwyr i sicrhau cadernid yn erbyn dulliau ymosod cyffredin cyn gynted â phosibl a rhoi mesurau diogelu mwy datblygedig ar waith lle bo hynny'n briodol. Ar gyfer Gweithredwyr Gwasanaethau Hanfodol a ddynodir o dan reoliadau NIS, mae hyn o leiaf yn golygu cyrraedd y safon sylfaenol a bennir gan yr Awdurdodau Cymwys perthnasol ar gyfer pob sector.

109. I gefnogi'r canlyniad hwn, byddwn yn adolygu gallu'r llywodraeth i ddal gweithredwyr CNI i gyfrif i sicrhau eu bod yn buddsoddi yn seiberddiogelwch systemau hanfodol ac yn rheoli eu risg yn effeithiol, gan gynnwys o'u cadwyni cyflenwi. Byddwn yn cryfhau'r fframwaith rheoleiddio, er mwyn gwella ei ddarpariaeth, ei bwerau a'i ystwythder i addasu, o fewn cyd-destun y risg diogelwch gwladol ehangach a'r bygythiad a'r dechnoleg sy'n newid yn gyflym. Bydd hyn yn dechrau gydag ymgynghoriad ar ddiwygiadau i reoliadau NIS, gweithredu'r fframwaith diogelwch newydd ar gyfer darparwyr telathrebu yn y DU a datblygu fframwaith rheoleiddio cymesur i sicrhau y bydd y system ynni clyfar a hyblyg y bydd ei hangen ar y DU i ddarparu Sero Net yn ddiogel ac yn gadarn yn erbyn bygythiadau seiber.

110. Ochr yn ochr â hyn, byddwn yn: gwella gallu rheoleiddwyr; buddsoddi mewn sgiliau i wella gallu gweithredwyr CNI i ddenu, i ddatblygu ac i gadw gweithwyr seiber proffesiynol (gweler y bennod ar Ecosystem Seiber y DU); a chefnogi rheolwyr i reoli risg y gadwyn gyflenwi drwy ymgysylltu rhagor â chyflenwyr hanfodol ac archwilio'r ystod lawn o ysgogiadau, o ganllawiau i gynigion deddfwriaethol a chaffael.

111. Mae'r seilwaith rydym yn defnyddio data arno yn ddiogel ac yn gadarn. Mae'r seilwaith hwn yn ased cenedlaethol hanfodol – un sy'n cefnogi ein heconomi, yn darparu gwasanaethau cyhoeddus ac yn sbarduno twf. Byddwn yn chwarae mwy o ran yn y gwaith o sicrhau bod data'n cael ei ddiogelu'n ddigonol pan fydd yn cael ei brosesu, yn cael ei drosglwyddo neu'n cael ei storio ar raddfa fawr, er enghraifft mewn canolfannau data allanol. Byddwn yn adeiladu fframwaith rheoli risg cryfach i sicrhau safonau diogelwch a chadernid uwch ar draws y sector ac yn gweithredu darpariaethau Deddf Diogelwch a Buddsoddi Cenedlaethol 2021 i sgrinio buddsoddiadau'n gryfach. Byddwn yn cryfhau ein gwaith gyda phartneriaid rhyngwladol i sicrhau nad yw mwy o fynediad a llifoedd data byd-eang yn cynyddu'r risgiau diogelwch sy'n wynebu'r DU, a byddwn hefyd yn mynd i'r afael â'r heriau diogelwch sy'n gysylltiedig â chasglu data torfol.

112. Byddwn hefyd yn ystyried pa mor hanfodol yw gwasanaethau seilwaith data'r DU o ran ategu'r economi a'i rôl mewn seilwaith cenedlaethol hollbwysig. Mae'r mesurau hyn yn cyd-fynd â'r ymrwymiadau a nodir yn y Strategaeth Data Genedlaethol a'r Adolygiad Integredig.

113. Mae mwy o fusnesau a sefydliadau yn y DU yn rheoli eu risgiau seiber yn rhagweithiol ac yn cymryd camau i wella eu seibergadernid. Byddwn yn darparu cymorth ac yn sbarduno newid mewn ymddygiad drwy ddatblygu cymhellion yn y farchnad sy'n hybu seiberddiogelwch effeithiol. Lle bo angen, bydd hyn yn cael ei ategu gan ddeddfwriaeth wedi'i thargedu i sicrhau bod risg seiber yn cael ei rheoli'n effeithiol gan y rheini sydd â'r cyfrifoldeb mwyaf i wneud hynny, a bod deddfwriaeth seiberddiogelwch y DU yn dal yn effeithiol yng ngoleuni risgiau a thechnolegau sy'n esblygu.

114. I gefnogi'r nodau hyn, byddwn yn gweithio fwyfwy gyda dylanwadwyr y farchnad (caffaelwyr, sefydliadau ariannol, buddsoddwyr, archwilwyr ac yswirwyr) i gymell arferion seiberddiogelwch da ar draws yr economi. Byddwn yn cynnig gwelliannau i adroddiadau corfforaethol ar gadernid i risgiau, gan gynnwys risgiau seiber. Bydd hyn yn rhoi gwell dealltwriaeth i fuddsoddwyr ac i gyfranddalwyr o sut mae cwmnïau'n rheoli ac yn lliniaru risgiau perthnasol i'w busnes. A byddwn yn parhau i hyrwyddo'r defnydd o achrediadau a safonau fel y cynllun ardystio Cyber Essentials a hyrwyddo ymgysylltiad ar lefel bwrdd â rheoli risgiau seiber.

115. Bydd deddfwriaeth a dargedir yn canolbwyntio'n bennaf ar sectorau lle mae effaith bosibl ymosodiadau seiber ar ei mwyaf, gan gynnwys darparwyr gwasanaethau hanfodol a digidol penodol, diogelu data yn yr economi ehangach, ac ar gyfer busnesau mwy. Bydd hyn yn ategu'r Cynllun ar gyfer Rheoleiddio Digidol, gan ganolbwyntio i ddechrau ar reoliadau sy'n llywodraethu diogelwch Rhwydweithiau a Systemau Gwybodaeth (NIS) – fel yr amlinellir uchod ac yn y bennod Technoleg a'r camau nesaf i ddiwygio trefn y DU ar gyfer diogelu data personol.

116. Bydd rhagor o fanylion sy'n amlinellu'r camau y byddwn yn eu cymryd i wella cadernid busnes a seiberddiogelwch ar draws busnesau a sefydliadau yn y DU yn cael eu nodi yn yr Adolygiad o Gymhellion a Rheoliadau Seiberddiogelwch.

117. Mae cyngor technegol, adnoddau hunan-gymorth a chynnyrch a gwasanaethau wedi'u sicrhau i wella seibergadernid yn hawdd i'w canfod a'u gwella'n barhaus, gyda phwyslais arbennig ar helpu dinasyddion, masnachwyr unigol a sefydliadau bach. Byddwn yn parhau i ddatblygu canllawiau a dulliau hunan-gymorth sy'n dechnegol gywir, yn amserol ac y gellir eu gweithredu drwy'r NCSC. Byddwn yn sicrhau bod negeseuon yn gyson, yn glir ac yn cael eu darparu drwy'r sianeli mwyaf effeithiol, boed hynny drwy ymgyrch Cyber Aware, gwefan NCSC, y llywodraeth, rhwydweithiau gorfodi'r gyfraith neu bartneriaethau â'r diwydiant; a byddwn yn sicrhau bod mwy o gymorth ar gael ar lefel leol. Drwy'r 'Hawl Ddigidol', byddwn yn parhau i ariannu cymwysterau Sgiliau Digidol Hanfodol yn llawn ar gyfer oedolion sydd eu hangen, gan sicrhau bod dysgwyr yn meddu ar y sgiliau digidol sylfaenol sydd eu hangen arnynt i fod yn ddiogel ac yn gyfrifol ar-lein. A byddwn yn helpu busnesau a sefydliadau i lywio drwy'r farchnad seiberddiogelwch gymhleth, gan ymestyn ein fframweithiau ar gyfer cynnyrch a gwasanaethau wedi'u sicrhau, a datblygu cynigion masnachol o amgylch Cyber Essentials a fydd yn ei gwneud yn haws i fusnesau bach gael gafael ar gyngor sylfaenol.

Elis Power, Swyddog Diogelu ac Atal Seiber, Uned Seiberdroseddau Rhanbarthol Tarian

Mae Uned Seiberdroseddau Rhanbarthol Tarian yn dîm amlddisgyblaethol o swyddogion heddlu a staff sydd ar secondiad o Heddluoedd Cymru. Eu nod yw cyfrannu at ddarparu amgylchedd seiber sy'n fwy diogel a saff yn Ne Cymru.

Mae'r Swyddog Diogelu/Atal Seiber, Elis Power, yn gweithio i'r tîm ymgysylltu:

"Mae'n ystrydeb ond does dim un diwrnod arferol ar yr uned. O ddydd i ddydd, gallwn fod yn gyfrifol am roi cyflwyniadau sy'n cynnwys cyngor i adrannau mewnol yr heddlu, neu sefydliadau allanol, i sicrhau eu bod yn deall yn iawn sut mae diogelu eu hunain a'u gweithle rhag bygythiadau seiber. Gallwn hefyd fod yn cyflwyno i bobl ifanc mewn ysgolion ar bynciau sy'n amrywio o ddiogelwch ar y rhyngrwyd i Ddeddf Camddefnyddio Cyfrifiaduron 1990. Rwy'n mynd i gyfarfodydd rheolaidd gydag asiantaethau partner a heddluoedd i drafod bygythiadau newydd a chanllawiau cysylltiedig i'n cynulleidfaoedd. Rwyf hefyd yn ymgysylltu â sefydliadau rydym wedi cael rhybuddion am wendidau ganddynt, yn cymryd rhan mewn ymgyrchoedd cenedlaethol, yn ymddangos mewn digwyddiadau a chynadleddau perthnasol, ac yn dod o hyd i amser i wella fy sgiliau, fy ngalluoedd a'm gwybodaeth yn gyson".

Amcan 3: Cryfhau cadernid ar lefel genedlaethol a sefydliadol er mwyn paratoi ar gyfer ymosodiadau seiber, ymateb iddynt ac adfer ar eu hôl

118. Er gwaethaf ymdrechion i ddeall y risg a chymryd camau ataliol, bydd rhai digwyddiadau'n dal i ddigwydd. Mae angen i ni gryfhau'r gallu i reoli ac ymateb i ddigwyddiadau ar draws pob sefydliad, er mwyn lleihau'r niwed a achosir a darparu gwell cymorth i ddioddefwyr. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

119. Mae'r ffordd mae'r DU yn rheoli ac yn cydlynu'r ymateb i ddigwyddiadau seiber sydd ag arwyddocâd cenedlaethol yn fwy effeithiol byth. Byddwn yn adeiladu ar brofiad y llywodraeth o ymateb i ddigwyddiadau seiber sylweddol, gan sicrhau bod y gwersi a nodir yn cael eu defnyddio i wella ein polisïau a'n prosesau. Byddwn yn rhannu ein profiad o reoli argyfyngau â phartneriaid rhyngwladol a'r diwydiant ac, yn ei dro, yn nodi arferion gorau o fannau eraill er mwyn gwella ein parodrwydd a'n prosesau. Byddwn yn sicrhau bod yr NCSC a thimau rheoli digwyddiadau asiantaethau gorfodi'r gyfraith yn meddu ar yr arbenigedd a'r adnoddau angenrheidiol i ymateb i'r ystod lawn o fathau o ddigwyddiadau sy'n esblygu a chydlynu ymateb cenedlaethol i fygythiadau blaenoriaeth.

120. Mae'n haws riportio digwyddiadau seiber ac mae dioddefwyr seiberdroseddau'n cael gwell cymorth. Bydd gwybodaeth riportio hefyd yn cael ei defnyddio i helpu i atal digwyddiadau yn y dyfodol a chefnogi asiantaethau gorfodi'r gyfraith i ymchwilio i seiberdroseddwyr, amharu arnynt a'u herlyn. I gefnogi hyn, byddwn yn darparu gwasanaeth riportio a dadansoddi twyll a seiberdroseddau cenedlaethol newydd yn lle Action Fraud erbyn 2025. Byddwn yn annog mwy o bobl i riportio digwyddiadau seiber mewn ffyrdd eraill, gan gynnwys drwy allu riportio busnes newydd yn Heddlu Dinas Llundain. Mewn sectorau sy'n cael eu rheoleiddio, byddwn yn galluogi rheoleiddwyr i fynnu bod ystod ehangach o ddigwyddiadau'n cael eu riportio, gan gynnwys 'digwyddiadau a fu bron â digwydd'. Bydd cyflwyno'r Uned Genedlaethol Gofal i Ddioddefwyr Troseddau Economaidd yn gwella'r gefnogaeth a'r arweiniad sydd ar gael i ddioddefwyr ar ôl profiad sy'n gallu achosi straen a niwed.

121. Mae'r Llywodraeth a CNI yn fwy parod i ymateb i ddigwyddiadau ac adfer ar eu hôl, gan gynnwys drwy gynllunio digwyddiadau'n well ac ymarfer rheolaidd. Byddwn yn helpu llywodraeth y DU a gweithredwyr CNI i ddod o hyd i'r gwasanaethau ymarferion seiber a rheoli digwyddiadau sydd eu hangen arnynt o'r farchnad drwy ehangu cynllun achrededig NCSC ar gyfer Ymateb i Ddigwyddiadau Seiber a chyflwyno cynllun newydd ar gyfer ymarfer.

122. Yn y llywodraeth, bydd galluoedd monitro a chanfod yn cael eu gwella mewn adrannau ac ar draws ystad ddigidol y llywodraeth. Byddwn yn sicrhau bod gwersi'n cael eu nodi a'u defnyddio i wella ein polisïau a'n prosesau; rhannu profiadau o reoli argyfyngau â phartneriaid rhyngwladol a diwydiant; a sicrhau bod gan ein timau rheoli digwyddiadau yr arbenigedd, y capasiti a'r gallu angenrheidiol i ymateb i'r ystod lawn o fathau o ddigwyddiadau sy'n esblygu.

123. Yn CNI byddwn yn nodi gofynion clir ar gyfer ymarfer a phrofi neu efelychu gwrthwynebwyr ar draws gweithredwyr CNI, ac yn ysgogi arloesedd a chydweithio mewn ymateb i ddigwyddiadau ac ymarfer, gan ystyried defnyddio modelau fel Canolfan Cydweithredu Seiber y Sector Ariannol. Ac fel rhan o'n huchelgeisiau ar dechnoleg (a amlinellir yn y bennod nesaf) byddwn yn sefydlu labordy cenedlaethol ar gyfer diogelwch technoleg weithredol fel canolfan ragoriaeth ar gyfer profi, ymarfer a hyfforddi ar dechnolegau diwydiannol hanfodol i feithrin gallu yn y maes hwn, ar y cyd â diwydiant, y byd academaidd a phartneriaid rhyngwladol.

124. Mae gan fusnesau a sefydliadau'r DU ddealltwriaeth gliriach o beth i'w wneud os bydd digwyddiad, pwy i'w ffonio, pwy all helpu a sut mae adfer. Byddwn yn gwella mynediad at hyfforddiant ac ymarferion, gyda chefnogaeth gwasanaethau'r diwydiant wedi'u sicrhau, gan gynnwys cynllun Ymateb i Ddigwyddiadau Seiber newydd a gwasanaeth Ymarfer Digwyddiadau Seiber. Byddwn yn sicrhau mynediad at gymorth gorfodi'r gyfraith cenedlaethol cyson i unigolion sy'n dioddef seiberdrosedd ac yn annog busnesau a sefydliadau bach i fanteisio ar gymorth lleol, fel eu Canolfan Seibergadernid ranbarthol.

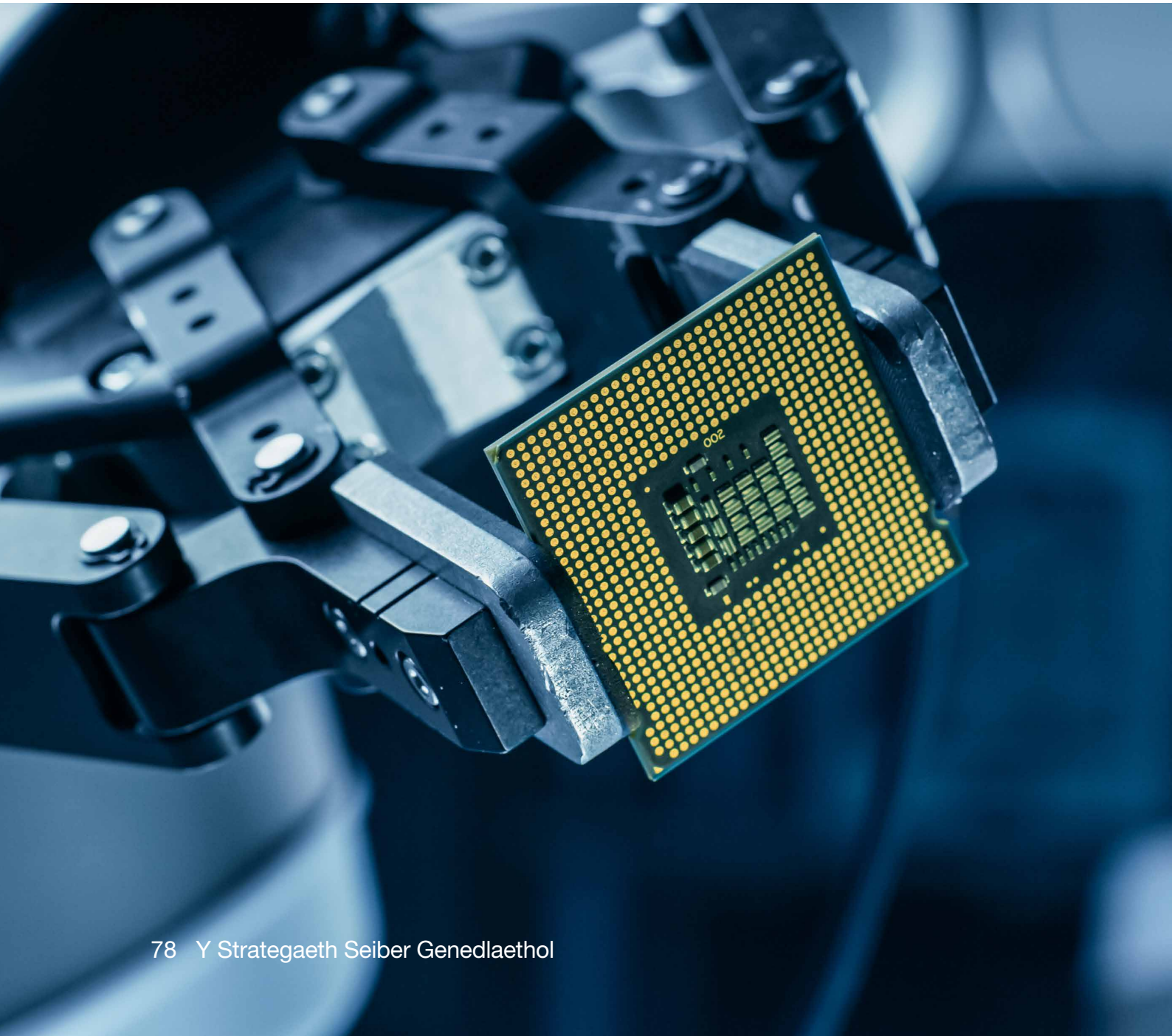
Daniel Ng, Prif Swyddog Gweithredol, CyberOwl

Cafodd CyberOwl fudd o raglen datblygu seiber y llywodraeth. Rydym yn dadansoddi ac yn monitro seiberddiogelwch ar gyfer asedau gweithredol yn y sectorau morol a CNI. Mae'r ymgyrch at gynaliadwyedd yn galw am fwy o gysylltedd a digidoleiddio asedau maes, gan eu hamlygu i risgiau seiber. Mae CyberOwl yn helpu gweithredwyr i ganfod a mapio eu hasedau, cael rhybudd cynnar o risgiau seiber a phrofi i'w hunain a rheoleiddwyr eu bod wedi sicrhau hynny. Rydym yn gweithio gyda gweithredwyr asedau morol mwyaf y byd ar draws EMEA ac Asia a'r Môr Tawel i wella cadernid y gadwyn gyflenwi logisteg llongau byd-eang. Yn 2021, rydym wedi cynyddu archebion 14 gwaith a dyblu ein gweithrediadau yn y DU a Singapore.

Jen Ellis, Is-lywydd Cymuned a Materion Cyhoeddus, Rapid7

Mae fy ngwaith yn cynnwys siarad ag arweinwyr a gweithwyr proffesiynol ym maes diogelwch mewn sefydliadau o bob maint a sector er mwyn deall yr heriau maen nhw'n eu hwynebu a cheisio dod o hyd i atebion i'w helpu i ddatblygu eu seiberddiogelwch. Rwy'n clywed yn gyson bod sefydliadau'n cael eu llethu a ddim yn gwybod ble i ganolbwyntio, sut mae dechrau arni, na sut mae symud ymlaen. Mae hefyd yn gallu bod yn anodd i staff technegol gael cefnogaeth gan yr arweinwyr. Mae cael strategaeth seiber glir, dryloyw a chyson gan y llywodraeth yn gallu helpu i fynd i'r afael â hyn. Mae'n rhoi rhywbeth i staff technegol gyfeirio ato fel rhan o'u trafodaethau gyda'r arweinwyr. Mae hefyd yn nodi meysydd ffocws craidd a llwybr posibl at aeddfedrwydd. Mae seiberddiogelwch yn dal yn hynod gymhleth ac yn ddi-ben-draw, ond gyda'r strategaeth seiber eang, mae mwy o ddealltwriaeth o'i bwysigrwydd a theimlad ein bod i gyd yn rhan o hyn gyda'n gilydd.

Colofn 3:
Mantais Technoleg



Cymryd yr awenau gyda'r technolegau sy'n hanfodol i seiberddiogelwch

125. Bydd rhai technolegau'n hollbwysig wrth lunio dyfodol seiberofod. Bydd gwledydd sy'n gallu sefydlu rôl arweiniol yn y technolegau hyn mewn sefyllfa well i ddylanwadu ar y ffordd maen nhw'n cael eu dylunio a'u defnyddio, yn fwy abl i ddiogelu eu diogelwch a'u mantais economaidd, ac yn manteisio'n gyflymach ar gyfleoedd i arloesi mewn galluoedd seiber. Wrth i dechnoleg ddod yn bwysicach o ran pŵer geowleidyddol, bydd y gystadleuaeth yn y maes hwn yn dwysáu.

126. I'r DU, bydd mynd ar drywydd mantais strategol drwy wyddoniaeth a thechnoleg, a'r mynediad at ddata y mae'n dibynnu arno, yn rhagamod ar gyfer cyflawni ein nodau ehangach fel pŵer seiber. Mae'r llywodraeth wedi cymryd camau mewn strategaethau blaenorol i ysgogi ymchwil ac arloesedd mewn technolegau seiberddiogelwch, fel drwy raglenni cyflymu ar gyfer busnesau newydd a'r Canolfannau Rhagoriaeth Academaidd mewn Ymchwil Seiberddiogelwch, ac i hybu datblygu dyfeisiau defnyddwyr sy'n 'ddiogel drwy ddylunio'. Fodd bynnag, mae angen dull mwy uchelgeisiol a rhagweithiol arnom yn awr i gynnal y gyfran mewn technolegau hanfodol ac i osgoi dibynnu gormod ar gystadleuwyr a gwrthwynebwyr.

127. Mae'r Adolygiad Integredig yn nodi cynlluniau i wneud y DU yn Uwch-bŵer Gwyddoniaeth a Thechnoleg a defnyddio gwyddoniaeth a thechnoleg i adeiladu ac i gynnal ein mantais strategol. Mae'r strategaeth hon yn cefnogi gwaith y Cyngor Gwyddoniaeth a Thechnoleg Cenedlaethol a'r Swyddfa Strategaeth Gwyddoniaeth a Thechnoleg wrth fynd ar drywydd y nod hwnnw, yn ogystal ag ategu strategaethau'r DU mewn meysydd fel Deallusrwydd Artiffisial, Technolegau Cwantwm a Data.

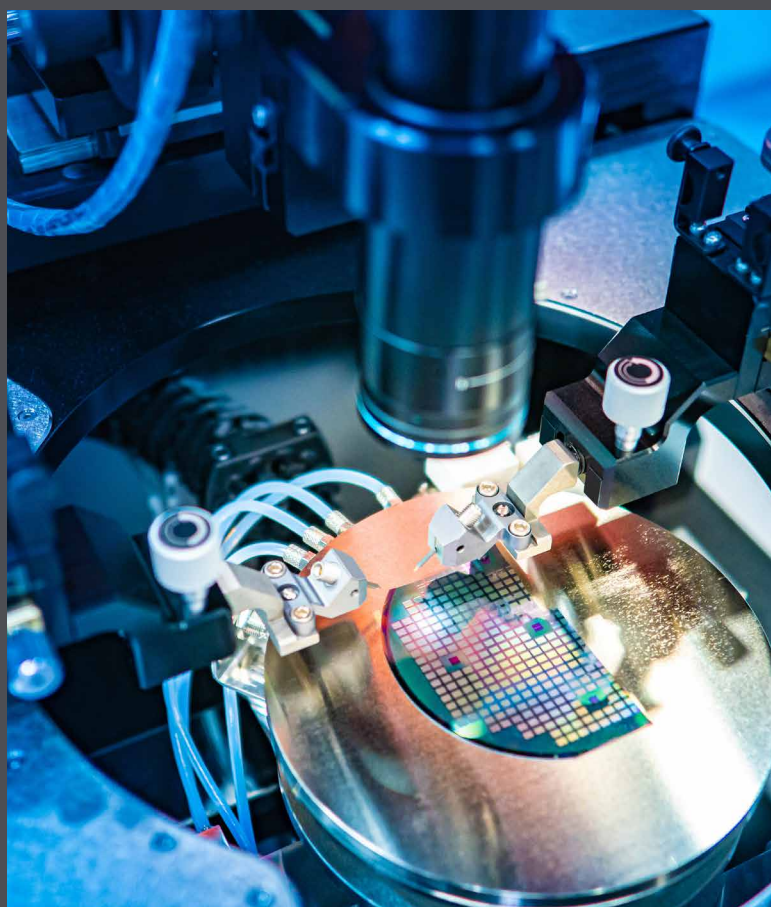
128. Byddwn yn cryfhau ein gallu, dan arweiniad arbenigedd technegol y Ganolfan Seiberddiogelwch Genedlaethol (NCSC) ac eraill ar draws y llywodraeth, i nodi'r meysydd technoleg sydd bwysicaf i'n pŵer seiber. Byddwn yn gwneud penderfyniadau strategol ar lefel genedlaethol ynghylch blaenoriaethau, gan weithio o fewn y fframwaith Perchen-Cydweithio-Mynediad sydd wedi'i nodi yn yr Adolygiad Integredig. Mewn ardaloedd dethol, byddwn yn buddsoddi yn y gweithgareddau ymchwil a datblygu a'r partneriaethau strategol sydd eu hangen i ddatblygu galluoedd domestig y DU, a phan fyddwn yn dibynnu ar farchnadoedd byd-eang, byddwn yn gweithio gyda'r diwydiant, rheoleiddwyr a phartneriaid rhyngwladol i hybu cadwyni cyflenwi amrywiol a dibynadwy, ac i siapio safonau i sicrhau bod technolegau'n ddiogel ac yn agored. Byddwn hefyd yn cryfhau gallu'r DU i fanteisio ar y symiau cynyddol o ddata a gwybodaeth sy'n cael eu cynhyrchu gan ac yn sbarduno arloesedd mewn technolegau newydd, gan adeiladu ar y fframwaith sydd wedi'i nodi yn y Strategaeth Data Genedlaethol er mwyn sicrhau'r manteision gorau posibl i'n heconomi ac i'n cymdeithas.

Technolegau sy'n hanfodol i Bŵer Seiber

Bydd amrywiaeth o dechnolegau presennol a newydd yn hanfodol i bŵer seiber y DU ac mae angen i ni allu rhagweld, asesu a gweithredu ar y datblygiadau hyn. Rydym yn disgwyl blaenoriaethu amrywiaeth o dechnolegau a rhaglenni wrth i ni gyflawni'r strategaeth, fel y rhai a nodir isod. Nid yw hon yn rhestr gynhwysfawr na statig a bydd ein blaenoriaethau'n parhau i esblygu drwy ymgynghori â diwydiant, y byd academaidd ac arbenigwyr technegol:

- Technoleg 5G a 6G, a mathau eraill o drosglwyddo data sy'n dod i'r amlwg
- Deallusrwydd artiffisial (AI), gan gynnwys yr angen i sicrhau systemau AI a'r potensial i ddefnyddio AI i wella seiberddiogelwch mewn amrywiaeth eang o raglenni fel monitro rhwydwaith
- Technoleg cadwyn atal a'i chymwysiadau fel cryptoarian a chyllid datganoledig
- Lled-ddargludyddion, sglodion microbrosesydd, pensaerniaeth microbrosesydd, a'u cadwyn gyflenwi, eu dyluniad a'u proses gweithgynhyrchu
- Dilysiad cryptograffig gan gynnwys ar gyfer rheoli hunaniaeth a mynediad a chynhyrchion cryptograffig sicrwydd uchel
- Y Rhyngrwyd Pethau a thechnolegau a ddefnyddir mewn amgylcheddau defnyddwyr, busnesau, diwydiannau a ffisegol fel lleoedd cysylltiedig
- Technolegau cwantwm, gan gynnwys cyfrifiadura cwantwm, synhwyro cwantwm a chryptograffeg ôl-gwantwm

Bydd y gwaith hwn yn cefnogi ac yn cyd-fynd â chyflawni nifer o strategaethau a chanlyniadau ar draws y llywodraeth, er enghraifft, y Strategaeth Data Genedlaethol, y Strategaeth Deallusrwydd Artiffisial Genedlaethol a'r Adolygiad Integredig, yn ogystal â'r canlyniadau sy'n canolbwyntio ar dechnoleg yn y Golofn hon.



Amcan 1: Gwella ein gallu i ragweld, asesu a gweithredu ar y datblygiadau gwyddoniaeth a thechnoleg sydd bwysicaf i'n pŵer seiber

129. Er mwyn meithrin a chynnal mantais gystadleuol mewn technolegau sy'n gysylltiedig â seiber, mae angen dull cydlynol, cadarn a chyson arnom i ganfod ac i ddadansoddi meysydd allweddol o wyddoniaeth a thechnoleg a blaenoriaethu ymdrechion cenedlaethol. Bydd hyn yn golygu y byddwn yn datblygu ein harbenigedd ymchwil a thechnegol yn y llywodraeth a'r byd academaidd hyd yn oed ymhellach. Byddwn yn integreiddio hyn â strwythurau newydd y llywodraeth ar gyfer cudd-wybodaeth a sganio'r gorwel gwyddoniaeth a thechnoleg, gan ddefnyddio dealltwriaeth arbenigwyr y diwydiant a defnyddio ein rhwydwaith tramor i ddeall blaenoriaethau a systemau partneriaid a chystadleuwyr rhyngwladol. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

130. Mae'r Llywodraeth yn gallu dadansoddi gwyddoniaeth a thechnoleg newydd yn well a deall y goblygiadau i bolisi a strategaeth seiber y DU. Byddwn yn ehangu ein gallu ymchwil gan gynnwys canolfan ymchwil gymhwysol newydd NCSC ym Manceinion, gan ganolbwyntio ar dechnoleg newydd mewn meysydd fel lleoedd cysylltiedig a thrafnidiaeth, gan weithio ochr yn ochr ag arbenigwyr yn Swyddfa'r Llywodraeth dros Wyddoniaeth ac mewn mannau eraill. Byddwn yn defnyddio arbenigedd o'r tu allan i'r llywodraeth, gan gefnogi'r pedwar Sefydliad Ymchwil Seiberddiogelwch a'r 19 Canolfan Ragoriaeth Academaidd mewn Ymchwil Seiberddiogelwch, ariannu Gwobrau Pathfinder i ymchwilwyr mewn pynciau blaenoriaeth, a defnyddio ein hôl troed dramor a'n partneriaethau rhyngwladol yn fwy effeithiol.

131. Mae'r ddealltwriaeth well hon yn cyfrannu'n gyflymach ac yn effeithiol at waith sganio'r gorwel ehangach, blaenoriaethu a phenderfyniadau'r llywodraeth, gan ganiatáu i ni fabwysiadu dull mwy rhagweithiol o fanteisio ar gyfleoedd a lliniaru risgiau. Byddwn yn sefydlu swyddogaeth sganio'r gorwel fewnol newydd i ragweld datblygiadau ym maes gwyddoniaeth a thechnoleg a'u goblygiadau seiber. Byddwn yn gwneud penderfyniadau mwy gwybodus i flaenoriaethu technolegau seiber allweddol, gan gyfeirio ymchwil a datblygu a datblygu polisïau a fydd o fudd i ddiogelwch y DU. Lle bo'n briodol, bydd hyn yn sail i benderfyniadau ehangach ar flaenoriaethau gwyddoniaeth a thechnoleg drwy'r Swyddfa Strategaeth Gwyddoniaeth a Thechnoleg a'r Cyngor Gwyddoniaeth a Thechnoleg Cenedlaethol.

Máire O'Neill, Prif Ymchwilydd y Ganolfan ar gyfer Technolegau Gwybodaeth Diogel (CSIT)

CSIT yw un o ganolfannau ymchwil technoleg prifysgol mwyaf y DU sy'n canolbwyntio ar seiberddiogelwch. Dan arweiniad y Prif Ymchwilydd yr Athro Máire O'Neill, cafodd ei dewis i fod yn un o Ganolfannau Arloesi a Gwybodaeth cyntaf y wlad yn 2009. Mae gwaith ymchwil, arloesi ac ymgysylltu llwyddiannus CSIT â'r diwydiant wedi arwain at dwf sylweddol yn ei enw da yn genedlaethol ac yn rhyngwladol dros y degawd diwethaf. Mae CSIT wedi bod yn ffactor hollbwysig yn llwyddiant Clwstwr Seiberddiogelwch Gogledd Iwerddon drwy gefnogi gweithgareddau deillio, tyfu busnesau cynhenid a Buddsoddi Uniongyrchol o Dramor yn y rhanbarth. O gychwyn llonydd yn 2009, mae sector seiber Gogledd Iwerddon bellach yn cyflogi 2,300 o bobl mewn 104 o gwmnïau, gan gynhyrchu £110 miliwn mewn cyflogau bob blwyddyn.

Amcan 2: Meithrin a chynnal mantais sofran a chysylltiedig o ran diogelwch technolegau sy'n hanfodol i seiberofod

132. Os oes gan y DU y potensial i sefydlu safle blaenllaw neu sicrhau mantais gystadleuol mewn meysydd allweddol o dechnoleg seiber, neu os bydd dibynnu ar ffynonellau cyflenwi nad ydynt yn gysylltiedig â'r farchnad yn peri risgiau diogelwch annerbyniol, byddwn yn ceisio datblygu ein sylfaen ddiwydiannol ddomestig. Bydd rhai meysydd lle mae angen inni gynnal gallu gwirioneddol sofran, ac eraill lle byddwn yn cydweithio â phartneriaid rhyngwladol neu'n chwilio am safle blaenllaw mewn un agwedd ar y farchnad. Bydd hyn yn gofyn am ddull cydlynol o ysgogi arloesedd ac ymchwil a datblygu ar y cyd â'r diwydiant a'r byd academaidd. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

133. Mae'r DU yn fwy llwyddiannus o ran troi ymchwil yn arloesedd ac yn gwmnïau newydd yn y meysydd technoleg sydd bwysicaf i'n pŵer seiber. Byddwn yn cefnogi academyddion ledled y DU i fasnacheiddio a rhoi eu hymchwil ar waith drwy fabwysiadu dull gweithredu sy'n fwy seiliedig ar herio ar y cyd â phartneriaid yn y diwydiant. Bydd hyn yn canfod syniadau sydd â'r potensial mwyaf ac yn ysgogi buddsoddiad gan gyllidwyr. A byddwn yn adeiladu ar y dull gweithredu a nodir yn y Strategaeth Arloesi, gan gefnogi'r gwaith o ddatblygu ecosystemau mwy sefydledig o amgylch technolegau allweddol, gan sicrhau bod mantais y DU yn fwy cadarn ac yn anoddach ei chopïo.

134. Mae'r DU mewn sefyllfa gryfach fyth fel arweinydd byd-eang ym maes dylunio microbrosesyddion diogel.[26] Byddwn yn adeiladu ar y rhaglen Diogelwch Digidol drwy Ddylunio sydd wedi datblygu technoleg newydd a mwy diogel ar gyfer sglodion cyfrifiadurol i ddiogelu meddalwedd rhag gwendidau. Byddwn yn defnyddio'r profiad hwn gyda phroseswyr Deallusrwydd Artiffisial i roi mantais ryngwladol i werthwyr yn y DU. A byddwn yn gweithio gyda'r Rhaglen Technolegau Cwantwm Genedlaethol i ddylunio model diogelwch ar gyfer cyfrifiaduron cwantwm ac i sicrhau bod cwmnïau'r DU yn arwain y byd gyda'r dechnoleg hon.

135. Ystyrir bod y DU yn arwain y byd ym maes ymchwil i ddiogelwch technolegau gweithredol a systemau rheoli diwydiannol hanfodol, ac yn ein gallu i'w profi a'u defnyddio yn y DU. Byddwn yn sefydlu labordy cenedlaethol ar gyfer diogelwch technoleg weithredol mewn partneriaeth â diwydiant a'r byd academaidd. Bydd yn cynnal rhaglenni ymchwil o'r radd flaenaf ac yn darparu'r cyfleusterau i'r llywodraeth, y fyddin, diwydiant a phartneriaid rhyngwladol ar gyfer ymarfer a phrofi'r technolegau hyn yma yn y DU. Ac fel cafodd ei gadarnhau yn Strategaeth Arallgyfeirio Cadwyn Gyflenwi Telathrebu 5G, byddwn yn sefydlu Labordy Telathrebu'r DU, gan ddod â'r llywodraeth a'r rheoleiddiwr ynghyd â'r diwydiant i gefnogi'r fframwaith diogelwch telathrebu newydd a helpu i gynyddu amrywiaeth gwerthwyr offer telathrebu yng nghadwyn gyflenwi'r DU.[27]

136. Mae'r llywodraeth mewn sefyllfa well i ddiogelu arloesedd ac eiddo deallusol y DU mewn technolegau seiber hanfodol yn erbyn gweithgarwch gelyniaethus, gan gynnal ein mantais gystadleuol.[28] Byddwn yn buddsoddi yn yr adnoddau a'r arbenigedd sydd eu hangen arnom i ddarparu arweinyddiaeth dechnegol ar ddiogelwch y technolegau hyn wrth iddynt ddatblygu, gan gynnwys cynghori ar risgiau buddsoddi uniongyrchol o dramor yn unol â nodau Deddf Diogelwch a Buddsoddi Cenedlaethol 2021. A byddwn yn parhau i weithio gyda busnesau a'r byd academaidd i greu amgylchedd dibynadwy mewn meysydd ymchwil a datblygu allweddol, ac yn datblygu mesurau cadarn i atal dwyn data ac eiddo deallusol.

---

[26] Microbrosesyddion yw ymennydd llawer o'r dyfeisiau rydym yn eu defnyddio heddiw. Maent ar gael ym mhobman, gan gynnwys mewn meysydd hollbwysig fel telathrebu, amddiffyn, gofal iechyd ac ar draws ein diwydiannau mawr. Mae datblygiadau technolegol ym maes dylunio systemau yn cael eu dal yn ôl ar hyn o bryd gan bryderon diogelwch, sy'n cael eu dwysáu gan gymhlethdod cynyddol y system.

[27] Yr Adran dros Dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon, 5G Supply Chain Diversification Strategy (2020)

[28] Gan ganolbwyntio'n benodol ar y sectorau hynny a nodir yn Neddf Diogelwch a Buddsoddi Cenedlaethol 2021: roboteg uwch, deallusrwydd artiffisial, cyfathrebu, caledwedd cyfrifiadura, dilysu cryptograffig a thechnolegau cwantwm

Diogelwch Digidol drwy Ddylunio

Mae saith deg y cant o'r gwendidau seiberddiogelwch presennol yn dangos nam yn y ffordd mae microbrosesyddion yn cael eu dylunio sydd wedi bod yn hysbys ers y 1970au. Mae'r microbrosesyddion hyn ar gael ym mhob dyfais ddigidol o setiau teledu i delathrebu. Mae'r llywodraeth wedi bod yn gweithio gyda'r sector technoleg i ddatrys hyn ac erbyn 2025 bydd dyluniad microbrosesyddion newydd ar gael ar gyfer ffonau clyfar, a rhestr gynyddol o ddyfeisiau eraill.

Mae newid dyluniad microbrosesyddion yn gofyn am fuddsoddiad a phartneriaethau byd-eang. Gyda'r DU yn arwain, a £70 miliwn o fuddsoddiad gan y llywodraeth, mae diogelwch yn cael ei ddylunio yn nyfeisiau'r dyfodol, gan leihau'r risg o ymosodiad seiber llwyddiannus yn sylweddol.

Ymchwiliwyd i'r dechnoleg arloesol yn y DU a chafodd ei datblygu yma hefyd. Mae arweinwyr technegol, gan gynnwys Microsoft, Google ac eraill, yn buddsoddi i ddod â'r manteision diogelwch newydd hyn i'w cynnyrch. Mae ymchwilwyr mewn prifysgolion ledled y DU yn gweithio i ddod o hyd i ffyrdd newydd o ddefnyddio'r dechnoleg ddiogel hon yn well ac mae'r llywodraeth yn cefnogi busnesau bach a chanolig yn y DU i ddod o hyd i farchnadoedd newydd ar gyfer cynnyrch sydd â'r diogelwch newydd hwn yn rhan ohonynt.

Phil Wilson, Cyfarwyddwr, Ymchwil a Datblygu yn The Hut Group

Mae The Hut Group yn fusnes e-fasnach sy'n canolbwyntio ar nwyddau defnyddwyr sy'n symud yn gyflym. Mae gennym dros 200 o wefannau sy'n rhedeg ar blatfform cyffredin gyda hyd at 3000 o archebion y funud i'w prosesu, felly mae diogelwch ein platfform a'n cwsmeriaid yn un o'n prif flaenoriaethau. Rydym yn buddsoddi llawer iawn o ymdrech i sicrhau y gellir cyfyngu ar unrhyw ymosodiad seiber a dyna pam ein bod mor gyffrous ynghylch posibilrwydd defnyddio technoleg Diogelwch Digidol drwy Ddylunio (DSbD) yn ein systemau. Byddai rhedeg ein systemau ar y microbrosesyddion newydd hyn, a ddatblygwyd mewn partneriaeth gwerth £180 miliwn rhwng y llywodraeth a'r diwydiant, yn gwneud ein systemau'n fwy cadarn ond byddai rheoli'r newid hwnnw'n gymhleth gan na allwn fabwysiadu technoleg newydd oni bai ei bod yn diwallu ein gofynion perfformiad. Mae wedi bod yn fraint cael bod y prosiect arddangos cyntaf ar gyfer y rhaglen DSbD ac rydym yn gobeithio elwa ar y diogelwch newydd hwn ar draws ein holl systemau yn y dyfodol agos.

Amcan 2a: Cadw menter Crypt-Allwedd genedlaethol gadarn sy'n diwallu anghenion cwsmeriaid, partneriaid a chynghreiriaid Llywodraeth Ei Mawrhydi, ac sydd wedi lliniaru ein risgiau mwyaf sylweddol yn briodol, gan gynnwys y bygythiad gan ein gwrthwynebwyr mwyaf galluog

137. Crypt-Allwedd yw'r term sy'n cael ei ddefnyddio i ddisgrifio sut mae'r DU yn defnyddio cryptograffeg i ddiogelu'r wybodaeth a'r gwasanaethau hanfodol y mae cymuned diogelwch genedlaethol a milwrol y DU yn dibynnu arnynt, gan gynnwys rhag ymosodiad gan ein gwrthwynebwyr mwyaf galluog. Mae'n sail i'n gallu i ddewis sut rydym yn defnyddio ein galluoedd diogelwch ac amddiffyn cenedlaethol. Er mwyn bod yn genedl Crypt-Allwedd sydd gyda'r gorau yn y byd, mae angen y sgiliau a'r technolegau cywir arnom yn y llywodraeth ac yn y sector preifat.

138. Byddwn yn parhau i fuddsoddi yn ein gallu mewn llywodraeth ac yn gweithio gyda'n diwydiant Crypt-Allwedd domestig i sicrhau bod y DU yn parhau i fod yn un o lond llaw o wledydd sy'n gallu datblygu Crypt-Allwedd sofran yn y dyfodol. Byddwn hefyd yn parhau i ddarparu arweinyddiaeth fyd-eang gyda Crypt-Allwedd, gan gynnwys cefnogi NATO fel cyflenwr deunyddiau allweddol. Bydd yr arweinyddiaeth hon yn arwain at ail gyfres o fanteision drwy gynnal diwydiant medrus iawn yn y DU a chadw ein cryfder mewn peirianneg gadarn iawn, gyda'r potensial i alluogi galluoedd cadarn newydd ar gyfer cyd-destunau sicrwydd uchel eraill fel seilwaith cenedlaethol critigol. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

139. Menter Crypt-Allwedd yn y DU sy'n fwy cadarn a diogel gyda sylfaen ddiwydiannol fwy cynaliadwy sy'n arwain y byd, sy'n cyflenwi'r ystod lawn o ddatrysiadau sydd eu hangen ar y DU ac sy'n allforio i'r partneriaid a'r cynghreiriaid sydd wedi cael eu dewis. Byddwn yn cyfuno galluoedd ac arbenigedd y llywodraeth a diwydiant yn fwy effeithiol, ac yn mabwysiadu dull mwy trylwyr a chenedlaethol o reoli'r fenter. Bydd hyn yn sicrhau ein bod yn datblygu'r sgiliau arbenigol penodol y mae arnom eu hangen.

140. Mae gan y DU wasanaethau a galluoedd Crypt-Allwedd cryfach mewn llywodraeth, sy'n gallu diwallu anghenion sy'n esblygu yn y DU ac ymhlith ein cynghreiriaid a sicrhau ein bod yn parhau i fod ar flaen y gad ym maes datblygu Crypt-Allwedd. Byddwn yn darparu arweinyddiaeth dechnegol gref i ddeall gofynion defnyddwyr ac i wella ein gwasanaethau craidd, gan gynnwys darparu deunyddiau allweddol a sicrwydd ynghylch cynnyrch a systemau. Byddwn hefyd yn trawsnewid gwasanaethau Crypt-Allwedd, gan harneisio technolegau newydd er mwyn iddynt fod yn fwy hyblyg ac anweledig.

141. Mae'r DU wedi datblygu ei harweinyddiaeth fyd-eang mewn Crypt-Allwedd a chynyddu'r allforion i'n partneriaid a'n cynghreiriaid. Byddwn yn cynnal ein rôl arwain yn y Five Eyes, NATO a phartneriaethau rhyngwladol eraill ac yn siapio'r gwaith o ddatblygu safonau sy'n cael eu cydnabod yn rhyngwladol er mwyn galluogi datrysiadau Crypt-Allwedd y DU i fod yn rhyngweithredol. A byddwn yn gweithio gyda'r diwydiant i fanteisio i'r eithaf ar gyfleoedd allforio.

Amcan 3: Sicrhau'r genhedlaeth nesaf o dechnolegau cysylltiedig, gan liniaru risgiau seiberddiogelwch dibyniaeth ar farchnadoedd byd-eang a sicrhau bod gan ddefnyddwyr y DU fynediad at gyflenwad amrywiol a dibynadwy

142. Dros y degawd nesaf byddwn yn parhau i weld pŵer cyfrifiadura, cysylltedd rhyngrwyd ac awtomeiddio yn cael eu gwreiddio mewn mwy a mwy o rannau o'n hamgylchedd, gan gynnwys gwrthrychau ffisegol a seilwaith ac, yn y tymor hirach, pobl eu hunain. Bydd hyn yn ymestyn cwmpas seiberofod ac yn cynyddu swmp y data a gynhyrchir yn sylweddol. Bydd y gallu i reoli data'n ddiogel ac yn saff yn dod yn bwysicach byth i sicrhau bod ein heconomi'n cael ei rhedeg yn ddiogel.

143. Lle bynnag y bo modd, mae angen i ni sicrhau bod y genhedlaeth nesaf o dechnolegau cysylltiedig yn cael eu dylunio, eu datblygu a'u defnyddio gyda diogelwch a chadernid mewn golwg ac fel rhan o ymdrech ar y cyd i gofleidio dull gweithredu 'diogel drwy ddylunio'. Mae natur fyd-eang cadwyni cyflenwi technoleg yn golygu y bydd angen i ni ddefnyddio'r holl ysgogiadau sydd ar gael i reoli risgiau dibyniaeth dechnolegol yn fwy gweithredol. Lle bo'n bosibl, byddwn yn ceisio sicrhau bod diogelwch yn cael ei ymgorffori; lle na allwn wneud hyn, byddwn yn rhoi mesurau cadarn ar waith i liniaru risg, gan gynnwys rheoleiddio domestig a chydweithredu rhyngwladol ar safonau. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

144. Mae cynnyrch defnyddwyr y gellir eu cysylltu sy'n cael eu gwerthu ledled y DU yn bodloni safonau seiberddiogelwch hanfodol. Byddwn yn cyflwyno ac yn gweithredu'r Bil Seilwaith Telathrebu a Diogelwch Cynnyrch er mwyn gallu gorfodi safonau diogelwch sylfaenol ym mhob cynnyrch defnyddwyr newydd y gellir eu cysylltu a werthir yn y DU. Byddwn yn cefnogi trawsnewidiad seiberddiogelwch i system ynni clyfar a hyblyg, gan gynnwys pwyntiau gwefru cerbydau trydan clyfar ac offer clyfar ynni. Byddwn yn gweithio gyda chyrff safonau, diwydiant a phartneriaid rhyngwladol i ddylanwadu ar y consensws byd-eang ar safonau technegol. A byddwn yn helpu sefydliadau yn y DU i gaffael, i ddefnyddio ac i reoli dyfeisiau sydd wedi'u cysylltu mewn ffordd fwy diogel, gan gynnwys drwy ganllawiau diogelwch newydd ar gyfer dyfeisiau mentrau sydd wedi'u cysylltu.

145. Mae'n rhaid i brif ddarparwyr gwasanaethau digidol, gan gynnwys cwmwl, meddalwedd, gwasanaethau a reolir a siopau apiau, ddilyn safonau diogelwch seiber gwell, gan helpu i ddiogelu sefydliadau a defnyddwyr rhag bygythiadau seiber. Byddwn yn cryfhau ac yn ehangu'r gwaith presennol o reoleiddio darparwyr gwasanaethau digidol ac yn rhoi hwb i allu Swyddfa'r Comisiynydd Gwybodaeth i sicrhau bod darparwyr digidol yn rheoli'r risgiau sy'n gysylltiedig â'u gwasanaethau mewn ffordd sy'n fwy rhagweithiol. Byddwn yn parhau i ymgysylltu â'r diwydiant, gan gynnwys y cwmnïau technoleg mawr, i harneisio arbenigedd yn y farchnad a sicrhau bod pawb yn chwarae rhan yn y gwaith o ddiogelu cadwyni cyflenwi digidol y DU. A byddwn yn arwain y gwaith o ddatblygu atebion polisi rhyngwladol sy'n canolbwyntio ar gyflenwyr digidol.

146. Mae'r DU ar flaen y gad o ran mabwysiadu technoleg lleoedd cysylltiedig yn ddiogel ac yn gynaliadwy er budd dinasyddion a busnesau. Mae gan leoedd cysylltiedig, sydd weithiau'n cael eu galw yn ddinasoedd clyfar, botensial i ddarparu manteision pendant i gymdeithas: rheoli traffig, lleihau llygredd ac arbed arian ac adnoddau. Fodd bynnag, mae'r rhyng-gysylltiad sy'n caniatáu i leoedd weithredu'n fwy effeithlon hefyd yn creu gwendidau seiber a'r potensial ar gyfer ymosodiadau seiber. Byddwn yn adeiladu ar egwyddorion diogelwch yr NCSC ar gyfer lleoedd cysylltiedig er mwyn lleihau'r risgiau i fusnesau, i seilwaith, i'r sector cyhoeddus ac i ddinasyddion.[29] Byddwn yn cryfhau gallu awdurdodau lleol a sefydliadau fel porthladdoedd, prifysgolion ac ysbytai, i brynu ac i ddefnyddio technoleg lleoedd cysylltiedig yn ddiogel. A byddwn yn adeiladu consensws rhyngwladol ar gyfer dull cyson ac effeithiol o ddiogelu lleoedd cysylltiedig.

147. Mae seiberddiogelwch wedi'i ddylunio i dechnolegau newydd eraill sy'n cael eu defnyddio yn y DU. Byddwn yn nodi rhaglenni technoleg newydd sy'n dod i'r amlwg ac sydd â'r potensial i greu risgiau seiberddiogelwch, ac yn sicrhau bod y DU ar flaen y gad o ran datblygu'r technolegau hyn yn ddiogel. Wrth i'r llywodraeth ystyried opsiynau ar gyfer gallu yn y DU o ran technoleg gefeilliaid digidol a thechnoleg 'seilwaith seiber' ehangach, byddwn yn sicrhau bod seiberddiogelwch wrth galon y broses o wneud penderfyniadau.[30] A byddwn yn cyflwyno cynllun sicrwydd i sicrhau bod y DU mewn sefyllfa gref ar gyfer cyflwyno ystod eang o gerbydau sydd wedi'u cysylltu a'u hawtomeiddio.[31]

[29] NCSC, Connected Places Cyber Security Principles (2021)
[30] Cyhoeddwyd yn y Innovation Strategy (2021)
[31] Y Broses Cerbydau Cysylltiedig ac Awtomataidd ar gyfer Sicrhau Diogelwch a Gwarchodaeth (CAVPASS)

Shadi A. Razak, Prif Swyddog Technegol a chyd-sylfaenydd Angoka

Mae cyhoeddi canllawiau ar leoedd cysylltiedig diogel gan y llywodraeth a'r defnydd cynyddol o gerbydau awtonomaidd yn tynnu sylw at bwysigrwydd diogelwch yn ein cymdeithas. Mae Angoka yn falch o ddeillio o raglen Cyflymu Seiber yr NCSC. Rydym yn darparu datrysiadau ar gyfer ystod eang o gymwysiadau, o seilwaith cenedlaethol critigol i symud ar dir a drwy'r awyr a mwy, gan sicrhau cadernid a sicrwydd diogelwch o'r dechrau i'r diwedd.

Cenhadaeth y cwmni yw sicrhau diogelwch a chadernid Dinasoedd Clyfar a symudedd, sy'n dod yn fwy cymhleth ac yn dibynnu ar rwydweithiau o ddyfeisiau cysylltiedig a chyfathrebu peiriant-i-beiriant. Mae ein datrysiad yn caniatáu creu parthau cymeradwy sy'n gweithredu diogelwch datganoledig, sy'n ddiogel o ran cwantwm, ac sy'n cael ei ddiweddaru'n ddynamig er mwyn darparu targed symudol i ymosodwyr drwy'r amser. Mae'n golygu bod perchnogion dyfeisiau yn gallu rheoli eu diogelwch yn llawn.

Tîm Angoka yn dangos eu datrysiad

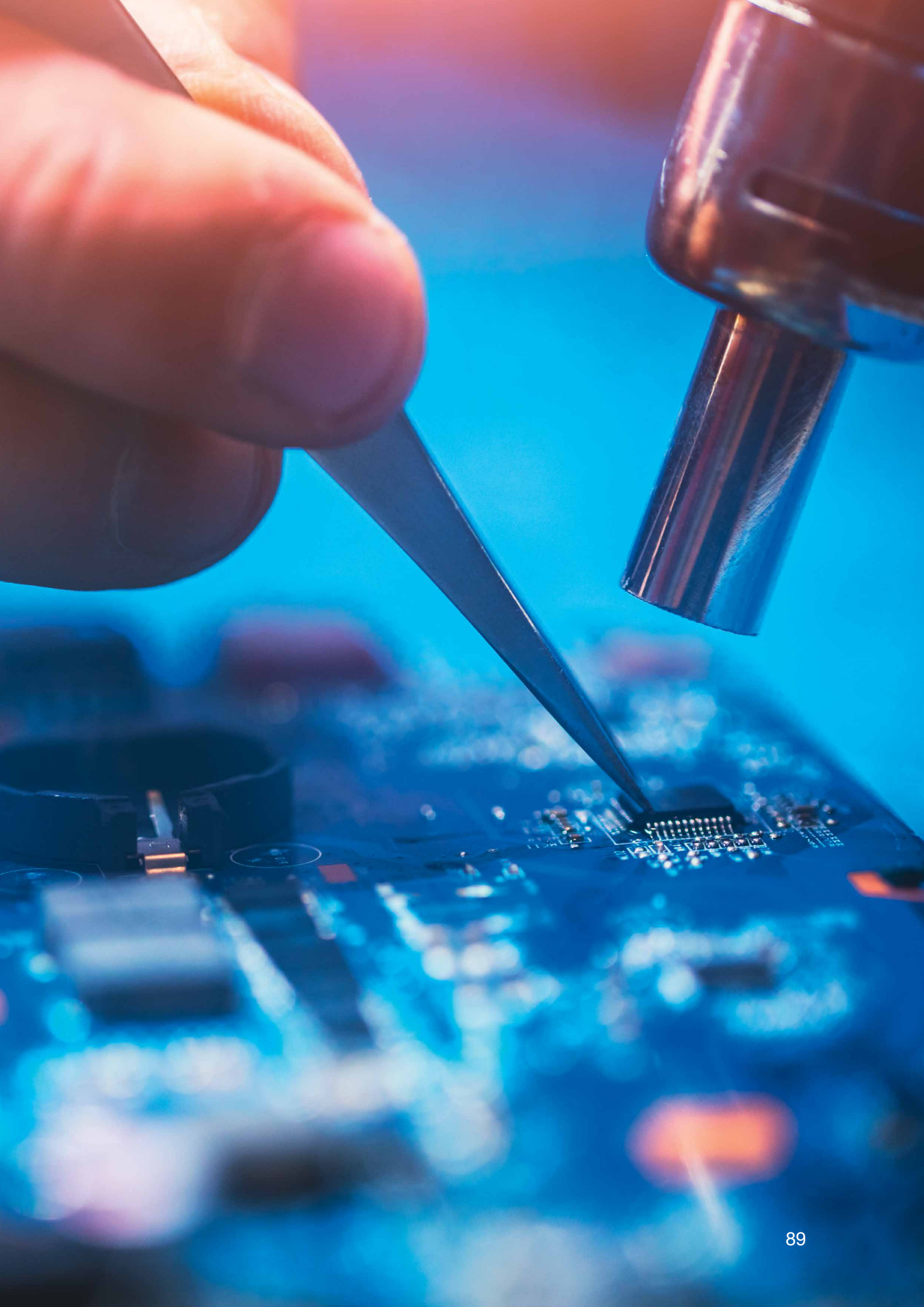
Amcan 4: Gweithio gyda'r gymuned sy'n cynnwys nifer o randdeiliaid i siapio'r gwaith o ddatblygu safonau technegol digidol byd-eang yn y meysydd blaenoriaeth sydd bwysicaf ar gyfer cynnal ein gwerthoedd democrataidd, sicrhau ein seiberddiogelwch, a hyrwyddo buddiannau strategol y DU drwy wyddoniaeth a thechnoleg

148. Mae safonau technegol digidol byd-eang yn rhan greiddiol o weithrediad y rhyngrwyd, rhwydweithiau telegyfathrebu a thechnolegau newydd. Gall y ffordd y cânt eu datblygu a'u defnyddio effeithio ar ein hamcanion seiberddiogelwch, ein ffyniant economaidd, a'n normau a'n gwerthoedd. Yn hanesyddol, mae'r safonau hyn wedi cael eu siapio gan y rheini sydd â'r pŵer mwyaf yn y farchnad ac mae rhwystrau sylweddol i fynediad sy'n atal rhai rhanddeiliaid pwysig, gan gynnwys busnesau bach a chanolig, academyddion, ac arbenigwyr eraill, rhag cymryd rhan. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

149. Mwy o gyfranogiad gan randdeiliaid niferus yn yr ecosystem safonau technegol digidol byd-eang. Byddwn yn atgyfnerthu cyfranogiad nifer o randdeiliaid mewn sefydliadau datblygu safonau allweddol ac yn arwain drwy esiampl gyda'n dirprwyaethau i'r Undeb Telathrebu Rhyngwladol. Byddwn yn hyrwyddo trafodaethau agored ar y prif dueddiadau ac ystyriaethau ar gyfer llunwyr polisïau drwy Fforwm Llywodraethu Rhyngrwyd y Cenhedloedd Unedig a fforymau eraill. A byddwn yn cryfhau'r cydlynu a'r rhannu gwybodaeth â phartneriaid rhyngwladol, gan gynnwys drwy'r Grŵp Pwyntiau Cyswllt ar gyfer Safonau Digidol, a sefydlwyd yn ystod llywyddiaeth G7 y DU.

150. Safonau technegol digidol byd-eang mewn meysydd blaenoriaeth ar gyfer y DU sy'n cael eu siapio'n fwy effeithiol gan werthoedd democrataidd, ystyriaethau seiberddiogelwch ac ymchwil ac arloesedd y DU mewn technolegau sy'n datblygu. Byddwn yn gweithio gyda diwydiant, y byd academaidd, arbenigwyr technegol a chymdeithas sifil mewn meysydd fel protocolau rhyngrwyd, rhwydweithiau'r dyfodol a Deallusrwydd Artiffisial (AI), i godi ymwybyddiaeth o ystyriaethau polisi cyhoeddus pwysig wrth ddatblygu safonau technegol. Byddwn yn treialu hyb safonau AI i gefnogi ymgysylltiad byd-eang y DU â safoni AI, fel y nodir yn y strategaeth AI Genedlaethol.

151. Bydd hyn oll yn cael ei gefnogi gan fecanweithiau cydlynu strategol yn y DU, fel y cynllun a nodir yn y Strategaeth Deallusrwydd Artiffisial Genedlaethol rhwng y llywodraeth, y Sefydliad Safonau Prydeinig (BSI) a'r Labordy Ffisegol Cenedlaethol. Bydd yr ymgysylltu hwn hefyd yn cefnogi ffyniant y DU drwy hyrwyddo safonau sy'n galluogi arloesi a hwyluso twf a chodi'r gwastad.



Colofn 4:
Arweinyddiaeth Fyd-eang

Hyrwyddo arweinyddiaeth a dylanwad byd-eang yn y DU ar gyfer trefn ryngwladol ddiogel a ffyniannus

152. Mae seiberofod rhydd, agored, heddychlon a diogel yn dal yn hanfodol i'n diogelwch a'n ffyniant i gyd, a bydd ymgysylltu rhyngwladol yn parhau i fod yn hanfodol er mwyn cyflawni holl amcanion strategaeth seiber y DU. Fodd bynnag, er mwyn ymateb i gyfnod o gystadleuaeth systemig, bydd y DU nawr yn ymgymryd â rôl arweinyddiaeth ryngwladol fwy gweithredol i hyrwyddo ein buddiannau a'n gwerthoedd mewn seiberofod. Bydd gweithgarwch y DU mewn seiberofod a'n harbenigedd seiber hefyd yn ganolog i gyflawni agenda polisi tramor ehangach y llywodraeth: byddwn yn eu defnyddio'n rhagweithiol i helpu i sicrhau trefn ryngwladol agored, ddiogel a ffyniannus.

153. Byddwn yn atgyfnerthu ein cynghreiriau craidd, gan weithio gydag ystod ehangach o bartneriaid, gan gynnwys diwydiant, cyrff safonau technegol byd-eang, cymdeithas sifil a'r byd academaidd fel gwlad sy'n datrys problemau ac yn rhannu'r baich. Byddwn yn buddsoddi mewn perthnasoedd dyfnach gyda phartneriaid yn Affrica ac Ardal Cefnfor yr India a'r Môr Tawel ac yn manteisio ar gyfleoedd ar gyfer cynghreiriau newydd, mwy ystwyth. Byddwn hefyd yn dal i wella ein pecyn cymorth diplomyddol, gan gysylltu ein dylanwad tramor â'n cryfderau domestig, gan fanteisio ar ein harbenigedd gweithredol a strategol ym maes cyfathrebu, ein rhaglenni sgiliau a'n partneriaethau economaidd fel grym byd-eang er lles. Mae ein dull gweithredu er budd diogelwch a ffyniant byd-eang, nid dim ond ein diogelwch a'n ffyniant ein hunain.

Amcan 1: Cryfhau seiberddiogelwch a seibergadernid partneriaid rhyngwladol a chynyddu gweithredu ar y cyd i amharu ar a rhwystro gwrthwynebwyr

154. Mae gweithredu ar y cyd a chadernid rhwng y naill a'r llall yn hanfodol i fynd i'r afael â bygythiadau uwch, ar yr un pryd â lleihau'r cymhellion i weithredwyr bygythiadau seiber gyflawni ymosodiadau yn erbyn y DU a'i phartneriaid. Byddwn yn cyflawni'r canlynol erbyn 2025:

155. Mae gan bartneriaid rhyngwladol y DU alluoedd cryfach, penderfyniad gwleidyddol, trefn lywodraethu, a systemau ar gyfer ymchwilio ac amharu ar fygythiadau seiber, yn ogystal ag ar gyfer meithrin gwytnwch. Bydd hyn wedi arwain at lai o fygythiad o dramor i ddinasyddion y DU. Byddwn yn rhoi blaenoriaeth i'n cymorth meithrin gallu seiber yn Nwyrain Ewrop, Affrica ac Ardal Cefnfor yr India a'r Môr Tawel, ac yn parhau i weithio gyda chynghreiriaid allweddol yn y Dwyrain Canol a Gogledd a De America. Byddwn yn datblygu cynnig technegol mwy integredig, llywodraeth gyfan, gyda mwy o fuddsoddiad mewn arbenigedd ym maes gorfodi'r gyfraith ac amddiffyn, gan fanteisio mwy ar ddiwydiant a'r byd academaidd yn y DU. Byddwn yn canolbwyntio ar ddiogelu seilwaith a chadwyni cyflenwi rhyngwladol hanfodol, hyrwyddo defnyddio technolegau digidol yn ddiogel a gweithio gyda phartneriaid yn y diwydiant i wneud hynny ar raddfa fawr.

156. Byddwn hefyd yn gwneud mwy i feithrin gallu sefydliadau cymdeithas sifil, gan alluogi trafodaeth seiliedig ar werthoedd am dechnoleg a chymdeithas a chreu mecanweithiau atebolrwydd lleol. A byddwn yn parhau i weithio gyda sefydliadau a phartneriaethau amlochrog effeithiol gan gynnwys y Cenhedloedd Unedig, Five Eyes, NATO, G7, yr Undeb Ewropeaidd, y Gymanwlad, y Sefydliad ar gyfer Cydweithrediad a Datblygiad Economaidd, y Fforwm Byd-eang ar Arbenigedd Seiber (GFCE), Fforwm ASEAN, Undeb Affrica a Banc y Byd.

157. Er mwyn gwella ein diogelwch ar gyfer buddiannau'r DU a dinasyddion dramor, byddwn hefyd yn datblygu ac yn cyflwyno ymgyrch hylendid seiber ryngwladol ar gyfer teithiau tramor y DU a fydd yn cael eu teilwra a'u darparu'n lleol. Y nod fydd codi cost gweithgarwch maleisus, fel hacio, dwyn data a dwyn eiddo deallusol a meddalwedd wystlo. Cyflwynir yr ymgyrch drwy ein diplomyddion, staff o'r wlad, y gymuned fusnes Brydeinig leol a gweithredwyr rhaglenni datblygu'r DU.

158. Cynghrair ryngwladol ehangach sy'n fodlon ac yn gallu rhoi canlyniadau mwy ystyrlon i wrthwynebwyr y DU. Byddwn yn gwella penderfyniad a gallu rhyngwladol drwy fwy o ymgysylltu diplomyddol, cydweithredu gweithredol, rhannu gwybodaeth ac ymarfer ar y cyd. Drwy weithio drwy sianeli polisi, gweithredol a gorfodi'r gyfraith, byddwn yn cynyddu effaith mesurau, fel sancsiynau seiber wedi'u targedu, yn ogystal â chanfod adnoddau newydd ar gyfer codi'r costau i'r rheini sy'n gyfrifol am fygythiadau seiber. Byddwn yn meithrin mwy o gyd-ddealltwriaeth ar draws grymoedd seiber y gwledydd allweddol cysylltiedig a'r gwledydd sy'n bartneriaid, ac yn integreiddio gweithrediadau seiber yn well i weithrediadau cysylltiedig ar draws pob maes: tir, môr, awyr, gofod a seiberofod.

159. A byddwn yn parhau i gefnogi datblygiad galluoedd seiberddiogelwch cynghrair NATO ar gyfer gweithredu ar y cyd cryfach, gan gynnwys cefnogi'r prosesau i integreiddio effeithiau seiber sofran a ddarperir yn wirfoddol gan y DU a rhai cynghreiriaid eraill, i weithrediadau ac ymgyrchoedd NATO.

Amcan 2: Llunio trefn lywodraethu fyd-eang i hyrwyddo seiberofod agored, heddychlon a diogel am ddim

160. Mae gwladwriaethau nad ydynt yn rhannu gwerthoedd y DU yn manteisio ar yr heriau a gyflwynir gan ryngrwyd rhydd ac agored i fwrw ymlaen â'u gweledigaethau awdurdodaidd ar gyfer seiberofod, o dan gochl diogelwch. Bydd y DU yn fwy rhagweithiol, gan weithio gyda'n cynghreiriaid a'n partneriaid i sicrhau bod rheolau a fframweithiau rhyngwladol yn datblygu yn unol â'n gwerthoedd democrataidd. Ein nod yw cefnogi twf economaidd cenedlaethol a byd-eang, gwella diogelwch ar y cyd, hybu defnydd cyfrifol o offer seiber ymosodol a sicrhau canlyniadau go iawn ar gyfer gweithgareddau maleisus ac anghyfrifol. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

161. Mae llywodraethu seiberofod a'r rhyngrwyd yn fyd-eang yn diogelu buddiannau a gwerthoedd y DU, gyda'r DU a'n partneriaid yn cael mwy o ddylanwad dros ddatblygu a gweithredu fframweithiau safonau a llywodraethu rhyngwladol. Byddwn yn fwy blaengar a rhagweithiol wrth lunio'r fframweithiau sy'n rheoli seiberofod er mwyn hybu twf economaidd a diogelwch byd-eang. Byddwn yn dylunio ac yn cyflwyno camau ymarferol sy'n chwalu'r ddadl ryngwladol ar ddefnyddio rheolau, normau ac egwyddorion mewn seiberofod ac yn ei symud at gonsensws ar gyfyngiadau effeithiol ar weithgarwch dinistriol sy'n dadsefydlogi. Byddwn yn gwneud hyn drwy sefydliadau rhanbarthol ac arbenigol allweddol gan gynnwys OSCE, ASEAN a'r GFCE ac yn ymgysylltu'n adeiladol â phroses y Cenhedloedd Unedig i ddatblygu cytuniad seiberdroseddu rhyngwladol newydd sy'n cyd-fynd â Chonfensiwn Budapest, gan sicrhau ei fod yn cryfhau cydweithrediad rhyngwladol ac yn dal i amddiffyn hawliau dynol.

162. Byddwn hefyd yn parhau i hyrwyddo Confensiwn Budapest ar seiberdroseddu, gan weithio gyda phartneriaid rhyngwladol i gyflwyno achos cryf iddo barhau i fod yn brif gytundeb rhyngwladol ar gyfer cydweithredu. A byddwn yn parhau i hyrwyddo a gwella prosesau sy'n cynnwys nifer o randdeiliaid ar gyfer llywodraethu'r rhyngrwyd, gan gynnwys ICANN ac yn Fforwm Llywodraethu'r Rhyngrwyd (IGF). Bydd yr ymdrechion hyn yn cael eu hategu gan ein gwaith i siapio safonau technegol digidol byd-eang (a ddisgrifir yn y bennod Technoleg) a'n gwaith i ehangu allforion seiberddiogelwch y DU (a nodir isod) a fydd hefyd yn helpu i wreiddio safonau'r DU yn ecosystemau seiber gwledydd eraill.

163. Mae'r rhan fwyaf o wledydd 'tir canol' yn cefnogi ac yn hyrwyddo gweledigaeth y DU ar gyfer seiberofod a dyfodol y rhyngrwyd, gan fynd i'r afael yn fwy llwyddiannus â dylanwad gwladwriaethau awdurdodaidd dros y system sy'n cynnwys nifer o randdeiliaid. Byddwn yn dangos ei bod yn bosibl mynd i'r afael â heriau mewn seiberofod heb fabwysiadu dulliau awdurdodaidd ar yr un pryd â galluogi arloesedd, datblygiad a thwf. Byddwn yn cefnogi gwledydd sy'n ymlafnio gyda digidoleiddio i adeiladu'r ystod lawn o arbenigedd cyfreithiol a chyfathrebu strategol sydd ei hangen arnynt i ymgysylltu â'r drafodaeth ryngwladol ac i weithredu fframweithiau y cytunwyd arnynt. Byddwn yn parhau i amlygu defnydd anghyfrifol o alluoedd seiber, gan feithrin ymddiriedaeth yn rhyngwladol. A byddwn yn parhau i ddangos agwedd agored a thryloyw at ein defnydd o alluoedd seiber ymosodol lle bynnag y gallwn, gan atgyfnerthu enw da'r DU fel grym er lles.

Amcan 3: Ysgogi ac allforio arbenigedd a galluoedd seiber y DU i roi hwb i'n mantais strategol a hyrwyddo ein buddiannau ehangach o ran polisi tramor a ffyniant.

164. Mewn ymateb i gystadleuaeth systemig a newid technolegol cyflym, bydd gweithgareddau a galluoedd seiber y DU yn cael eu hystyried ochr yn ochr â ffynonellau pŵer cenedlaethol eraill i gynyddu ein mantais strategol a hyrwyddo ein nodau o ran polisi tramor a ffyniant. Ein nod yw sicrhau trefn ryngwladol lle gall cymdeithasau ac economïau agored ffynnu ac amddiffyn hawliau dynol, ar yr un pryd â hybu ffyniant gartref. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

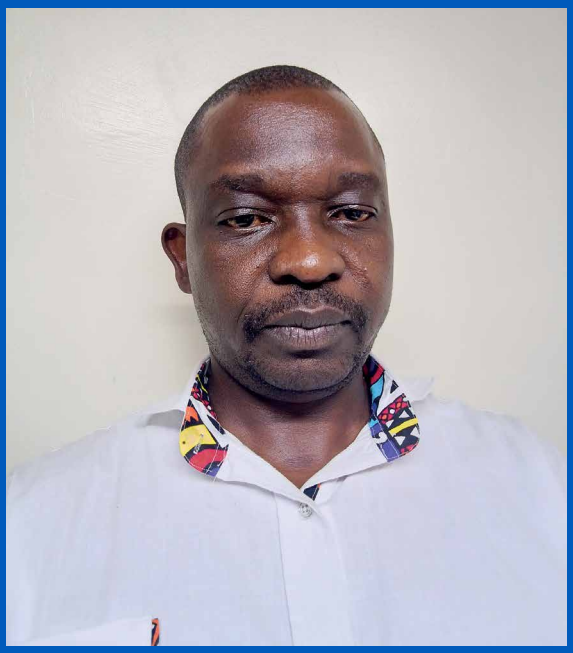
165. Mae ein gweithgarwch mewn seiberofod ac mewn perthynas ag ef wedi gwella sefydlogrwydd byd-eang ac wedi diogelu'r system ryngwladol sy'n seiliedig ar reolau, cymdeithasau agored a systemau democrataidd lle maen nhw'n cael eu tanseilio. Byddwn yn cyflwyno ymgyrch ryngwladol seiliedig ar werthoedd i hyrwyddo hawliau dynol, amrywiaeth a chydraddoldeb rhwng y rhywiau wrth ddylunio, datblygu a defnyddio seiberofod. Ymhlith pethau eraill bydd hyn yn cynnwys mynd i'r afael ag achosion o gau'r rhyngrwyd, rhagfarn mewn algorithmau Deallusrwydd Artiffisial a chynyddu diogelwch ar-lein. Byddwn yn cystadlu'n fwy effeithiol i ddiogelu gwerthoedd, systemau a phrosesau democrataidd ac yn cryfhau'r system ryngwladol sy'n seiliedig ar reolau (gan gynnwys y Cenhedloedd Unedig, Sefydliad Iechyd y Byd a'r system fasnachu fyd-eang) drwy fuddsoddi ymhellach yn ein rhwydwaith o swyddogion seiber sy'n ymestyn ar draws chwe chyfandir. Byddwn yn gwella ein defnydd o gyfathrebu strategol i hyrwyddo cydweithio ymchwil yn y DU a rhaglenni cyfnewid academaidd ac yn helpu i sicrhau bod syniadau'r DU yn cael eu trosi'n gymwysiadau ymarferol.

166. Mae'r DU yn un o'r 3 prif allforwr byd-eang sy'n cynnig datrysiadau seiber ac arbenigedd seiber, gyda'n diwydiant seiber yn cael ei ystyried fel y prif ddarparwr datrysiadau seiberddiogelwch ar gyfer llywodraethau tramor a chleientiaid masnachol mawr. Byddwn yn arddangos seiberddiogelwch gorau'r DU drwy ymgysylltu mwy gweithredol â llywodraethau'n rhyngwladol, dan nawdd Rhaglen Llysgenhadon Seiberddiogelwch y DU a'n rhwydwaith rhyngwladol. Byddwn yn cefnogi cwmnïau ledled y DU ar bob cam o'r llwybr arloesi ac allforio i ddod yn allforwyr cymwys a denu mewnfuddsoddiad a darparu mwy o gymorth i fusnesau bach a chanolig, gan gynnwys drwy Uwch-adran Allforio newydd.[32] [33] Ochr yn ochr â'n gwaith drwy'r Bartneriaeth Twf Seiber ac ymdrechion eraill a amlinellir yn y bennod ar Ecosystem Seiber y DU, byddwn hefyd yn datblygu Swyddfa Ymgyrch Gallu Seiber newydd i ddarparu cymorth mwy strwythuredig a chydlynol i ymgyrchoedd allforio mawr.

[32] Wedi'i ddisgrifio yn UK Innovation Strategy (2021)

[33] Mae Uwch-adran Allforio Allforion Amddiffyn a Diogelwch y DU (UKDSE) yn hyb dysgu a datblygu ar-lein sydd wedi'i anelu at fusnesau bach a chanolig yn y sector amddiffyn a diogelwch gyda modiwlau penodol ar gyfer cwmnïau seiberddiogelwch. Mae cofrestru ar gyfer yr Uwch-adran yn rhoi mynediad at raglen o fodiwlau dysgu sy'n seiliedig ar y cwricwlwm ac, yn ogystal, gwybodaeth werthfawr am ddigwyddiadau a gweithgareddau arfaethedig Allforion Amddiffyn a Diogelwch y DU.

Charles Juma, Rhaglen Mynediad Digidol y DU yn Nairobi



Charles Wesonga Juma ydw i. Rwy'n arwain, yn siapio ac yn darparu seiberddiogelwch, datblygiad digidol, cynhwysiant ac entrepreneuriaeth fel rhan o Raglen fyd-eang a thrawslywodraethol Mynediad Digidol y DU yn Kenya. Rwyf hefyd yn cefnogi prosiectau ategol o dan Bortffolio Seiber y Gronfa Gwrthdaro, Sefydlogrwydd a Diogelwch (CSSF). Ni ellir gorbwysleisio pwysigrwydd diogelwch ar-lein, diogelwch, diogelu data a defnyddio seiberofod yn gyfrifol. Fel rydym wedi'i ddysgu o bandemig COVID-19, gall diogelwch a hylendid ar-lein fod yr un mor bwysig ag iechyd a hylendid y cyhoedd. Rwy'n frwd dros sicrhau bod pawb yn cael ei ddiogelu rhag bygythiadau a niwed ar-lein fel rhan o bŵer seiber cyffredinol llywodraeth y DU.

Sara Merchant, Swyddog Seiber yn Llysgenhadaeth Prydain, Tbilisi

Sara ydw i ac rwy'n gweithio yn Llysgenhadaeth Prydain fel Swyddog Seiber, gan weithio'n agos gyda Llywodraeth Georgia a NCSC y DU. Mae fy ngwaith o ddydd i ddydd yn amrywio o ymgysylltu gwleidyddol, i gefnogi'r gwaith o roi'r strategaeth seiber newydd ar waith, i ysgogi arbenigwyr y DU i gynyddu gallu technegol Georgia. Mae'n fraint cael bod ar flaen y gad o ran rhannu arbenigedd y DU a chefnogi Georgia i feithrin cadernid yn erbyn bygythiadau seiber. Fel gwlad sydd, yn anffodus, â llawer iawn o brofiad o ddioddef gweithgarwch gelyniaethus gwladwriaethol, mae llawer y gallwn ei ddysgu yma yn Georgia. Mae ein gwaith yn ein gwneud yn gryfach, yn fwy cadarn ac yn fwy gwybodus.

Colofn 5:
Gwrthsefyll Bygythiadau

Canfod, amharu a rhwystro ein gwrthwynebwyr er mwyn gwella diogelwch y DU mewn seiberofod a thrwyddo

167. Mae natur y bygythiad a wynebwn yn gymhleth. Rydym yn poeni am fygythiadau mewn seiberofod (er enghraifft i'n gweithgareddau ar-lein), bygythiadau i'r DU ac i bartneriaid drwy seiberofod (er enghraifft, i seilwaith cenedlaethol hanfodol wedi'i rwydweithio yn y DU), a bygythiadau i weithrediad seilwaith seiber rhyngwladol sylfaenol. Mae'r holl fygythiadau hyn yn gallu effeithio ar argaeledd gwasanaethau y mae pobl yn dibynnu arnynt, neu ar gyfrinachedd neu gywirdeb data a gwybodaeth sy'n mynd drwy'r systemau hynny. Mae sylfeini ein dull gweithredu i fynd i'r afael â'r bygythiad yn cynnwys hyrwyddo seibergadernid fel yr amlinellir yn gynharach yn y ddogfen hon. Mae'r bennod hon yn canolbwyntio ar sut byddwn yn codi costau a risgiau ymosod ar y DU mewn seiberofod a sicrhau ein bod yn cyflawni ein potensial llawn fel pŵer seiber.

168. Ers Strategaeth Seiberddiogelwch Genedlaethol 2016-2021, rydym wedi trawsnewid ein dull o liniaru'r bygythiad. Rydym wedi sefydlu galluoedd canfod a dadansoddi bygythiadau seiber o'r radd flaenaf fel rhan o'r Ganolfan Seiberddiogelwch Genedlaethol (NCSC). Mae'r NCSC yn gweithio gyda phartneriaid ar draws y sector cyhoeddus a phreifat, gartref a thramor, i ganfod ac i ymateb i fygythiadau a digwyddiadau. Fel rhan o'r gymuned cudd-wybodaeth ehangach, mae'r NCSC hefyd wedi gallu rhoi gwybod i lunwyr polisïau am briodoli ymosodiadau yn erbyn buddiannau'r DU, sy'n rhan hollbwysig o'n dull o atal bygythiadau seiber. Rydym wedi buddsoddi'n sylweddol yn ein galluoedd seiber ymosodol, drwy'r Rhaglen Seiber Ymosodol Genedlaethol, ac nawr drwy'r Llu Seiber Cenedlaethol (NCF) newydd. Rydym hefyd wedi datblygu ymateb gorfodi'r gyfraith cenedlaethol integredig dan arweiniad yr Asiantaeth Troseddu Cenedlaethol (NCA), ac rydym wedi ceisio amharu ar weithgarwch gelyniaethus a throseddol mewn seiberofod a chynyddu cost hynny. Rydym wedi creu galluoedd canfod ac asesu bygythiadau o'r radd flaenaf gyda'r gallu i drosi'r hyn a ganfyddir yn fesurau lliniaru effeithiol ar draws y sector cyhoeddus a phreifat. Ac rydym wedi datblygu trefn sancsiynau seiber awtonomaidd fel ffordd arall o roi costau ar weithredwyr gelyniaethus. Ar y cyd, mae ein hymgysylltiad diplomyddol, yr NCSC, ein hasiantaethau diogelwch a chudd-wybodaeth, yr NCA, asiantaethau gorfodi'r gyfraith yn ehangach a'r NCF wedi lleihau'r effaith go iawn a achosir gan fygythiadau, drwy gymryd camau i wrthsefyll gwrthwynebwyr yn uniongyrchol, helpu i atal ymosodiadau, a lleihau niwed.

169. Ond mae'r bygythiadau hefyd yn fwy soffistigedig, cymhleth a difrifol; ac yn y bôn nid yw ein hymdrechion wedi newid calcwlws risg ymosodwyr sy'n parhau i lwyddo i dargedu'r DU a'i buddiannau. Mae ymosodiadau seiber yn erbyn y DU yn cael eu cymell gan ysbïo, buddiannau troseddol, masnachol, ariannol a gwleidyddol, difrod a thwyllwybodaeth. Mae ymosodwyr yn datblygu galluoedd sy'n osgoi mesurau lliniaru; mae offer seiber sy'n fwy soffistigedig a galluogwyr cysylltiedig bellach yn nwyddau mewn diwydiant sy'n tyfu, gan leihau'r rhwystrau sy'n atal pob math o weithredwyr maleisus rhag cael mynediad. Ac mae gwobrau'n cynyddu wrth i allu gweithredwyr barhau i dyfu gan eu galluogi i ddwyn ac amgryptio data gwerthfawr a chael taliadau meddalwedd wystlo, gan amharu ar fusnesau a gwasanaethau cyhoeddus allweddol. O ganlyniad, mae ymosodwyr yn elwa fwyfwy yn ariannol, yn ecsbloetio preifatrwydd a rhyddid i lefaru, ac yn ceisio dylanwadu ar ddigwyddiadau drwy dwyllwybodaeth.

170. Felly, bydd dull gweithredu'r DU nawr yn symud at sylfaen ymgyrchu fwy integredig a pharhaus a fydd yn golygu gwneud defnydd rheolaidd, integredig a chreadigol o'r ystod lawn o ysgogiadau a galluoedd sydd ar gael i osod costau ar ein gwrthwynebwyr, mynd ar drywydd a tharfu ar ddrwgweithredwyr a rhwystro ymosodiadau yn y dyfodol. Elfennau ategol allweddol y dull hwn fydd:

- parhau i ddatblygu'r NCF fel y cam nesaf yng ngallu'r DU i gynnal gweithrediadau seiber ymosodol yn erbyn ei gwrthwynebwyr
- ymgyrchoedd traws-lywodraethol wedi'u teilwra i fynd i'r afael â bygythiadau i'r DU – gan ddefnyddio ein hadnoddau cyfathrebu diplomyddol, milwrol, cudd-wybodaeth, gorfodi'r gyfraith, economaidd, cyfreithiol a strategol
- buddsoddiad newydd i alluogi asiantaethau gorfodi'r gyfraith i fynd ar drywydd ymchwiliadau ar raddfa fawr ac yn gyflym ac i gynnal mantais dechnegol dros ein gwrthwynebwyr er mwyn atal a chanfod troseddwyr difrifol a'r gwasanaethau galluogi y maent yn dibynnu arnynt
- cam mawr ymlaen o ran rhannu data ar draws y llywodraeth a'r diwydiant fel yr amlinellir yn y bennod ar Gadernid

171. Mae seiberofod yn cyflwyno cyfleoedd i'r DU, gan greu ffyrdd newydd o fynd ar drywydd ein buddiannau cenedlaethol. Er enghraifft, mae gweithrediadau seiber ymosodol yn cynnig amrywiaeth o fesurau hyblyg, graddadwy a dad-waethygol i ni a fydd yn helpu'r DU i gynnal ein mantais strategol ac i gyflawni blaenoriaethau cenedlaethol, yn aml mewn ffyrdd sy'n osgoi'r angen i roi unigolion mewn perygl o niwed corfforol.

172. Byddwn yn parhau i ddatblygu a buddsoddi yn ein galluoedd seiber ymosodol, drwy'r NCF. Bydd yr NCF yn trawsnewid gallu'r DU i herio gwrthwynebwyr mewn seiberofod ac yn y byd go iawn, er mwyn diogelu'r wlad, ei phobl a'n ffordd o fyw. Bydd y galluoedd hyn yn cael eu defnyddio'n gyfrifol fel grym er lles ochr yn ochr ag ysgogiadau pŵer diplomyddol, economaidd, cyfiawnder troseddol a milwrol. Byddant yn cael eu defnyddio i gefnogi ac i ddatblygu ystod eang o flaenoriaethau'r llywodraeth sy'n ymwneud â diogelwch gwladol, lles economaidd, ac i gefnogi'r gwaith o atal a chanfod troseddau difrifol.

Amcan 1: Canfod, archwilio a rhannu gwybodaeth am weithredwyr a gweithgareddau seiber maleisus sy'n gysylltiedig â gwladwriaethau, troseddu neu feysydd eraill er mwyn amddiffyn y DU, ei buddiannau a'i dinasyddion

173. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

174. Mae gan y llywodraeth ddealltwriaeth gynhwysfawr o'r galluoedd seiber sydd gan weithredwyr seiber gwladwriaethol, troseddol neu rai maleisus eraill ac o'u bwriad strategol mewn perthynas â'r DU. Byddwn yn cynnal ac yn tyfu'r buddsoddiadau sylweddol a wnaed o dan strategaeth 2016 yn yr asiantaethau cudd-wybodaeth a gorfodi'r gyfraith er mwyn deall y bygythiad seiber. Yn benodol, byddwn yn cynyddu gallu asiantaethau gorfodi'r gyfraith i ddeall a mynd i'r afael â'r bygythiad o seiberddiogelwch, gan gynnwys ei gysylltiadau â gwladwriaethau a bygythiadau domestig a rhyngwladol eraill a'i galluogwyr technolegol, gan ein helpu i ddatblygu ymatebion polisi mwy effeithiol. Byddwn yn gwella sut rydym yn cydlynu'r gwaith o ganfod bygythiadau ar draws y llywodraeth, gyda strategaeth ecsbloetio a mynediad at ddata ar y cyd ar draws yr asiantaethau cudd-wybodaeth a gorfodi'r gyfraith. A byddwn yn canolbwyntio mwy fyth ar ddeall bwriad a meini prawf gwneud penderfyniadau ein gwrthwynebwyr a'r effaith y mae ein gweithgareddau'n ei chael arnynt, gan gynnwys sut mae unigolion yn dod yn seiberdroseddwyr a pha gamau y gallwn eu cymryd i atal hyn rhag digwydd.

175. Bydd ein gwaith i alluogi riportio digwyddiadau a throseddau seiber yn gyflymach ac yn haws, a amlinellir yn y bennod ar Gadernid, hefyd yn helpu i gyflawni'r canlyniad hwn.

176. Ymchwilir i'r rhan fwyaf o'r bygythiadau mwyaf difrifol gan weithredwyr sy'n gysylltiedig â gwladwriaethau, troseddu neu feysydd eraill, gan ddefnyddio'r holl ffynonellau gwybodaeth sydd ar gael a chrynhoi arbenigedd ar draws llywodraeth, asiantaethau gorfodi'r gyfraith a'r sector preifat. Byddwn yn adeiladu galluoedd cudd-wybodaeth, gweithredol a thechnegol rhwydwaith seiber asiantaethau gorfodi'r gyfraith y DU. Byddwn yn buddsoddi yng ngallu cudd-wybodaeth yr NCA, a ddefnyddir i dargedu grwpiau troseddu cyfundrefnol, y fenter datblygu cudd-wybodaeth ranbarthol, a fydd yn gwella mynediad a symudiad cudd-wybodaeth ledled y DU, a'r sgiliau a'r gallu sydd eu hangen ar orfodi'r gyfraith i ymchwilio i ac amharu ar droseddau seiber a digidol.

177. Bydd ymchwiliadau'n cael eu hategu gan gudd-wybodaeth o bob ffynhonnell ac yn defnyddio sgiliau a gwybodaeth ar draws y sector preifat, gan gynnwys drwy helpu busnesau i rannu data'n haws ag asiantaethau gorfodi'r gyfraith. A byddwn yn parhau i weithredu argymhellion HMICFRS ar yr ymateb plismona i seiberdroseddu er mwyn sicrhau bod y rhwydwaith seiberdroseddu ar lefel genedlaethol, ranbarthol a lleol yn parhau i fod yn gadarn.[34]

[34] Arolygiaeth Cwnstabliaeth a Gwasanaethau Tân ac Achub Ei Mawrhydi

178. Mae gwybodaeth a data am y bygythiad yn cael eu rhannu'n rheolaidd ar raddfa fawr ac yn gyflym ac mae'r rheini sy'n cael yr wybodaeth a'r data hynny mewn sefyllfa well i weithredu. Mae'r NCSC wedi treialu amrywiaeth o gynlluniau i greu cymunedau mwy effeithiol o amddiffynwyr rhwydwaith, ar draws amrywiaeth eang o sectorau, sydd nid yn unig yn derbyn ac yn gallu rhannu gwybodaeth am fygythiadau, ond sy'n fwyfwy abl i'w defnyddio er budd pawb. Byddwn yn ehangu'r gwaith hwn, gan ganolbwyntio i ddechrau ar helpu'r llywodraeth i amddiffyn ei hun yn well, gyda chefnogaeth Canolfan Cydlynu Seiber y Llywodraeth (a ddisgrifir yn y bennod ar Gadernid). Mae Canolfan Cydweithredu Seiber y Sector Ariannol eisoes yn arwain y ffordd yn y sector preifat.[35]

179. Mae'r NCSC hefyd yn ymchwilio i ffyrdd o olrhain bygythiadau sy'n dod i'r amlwg ac yn parhau i weithio gyda Sefydliad Alan Turing i weld a oes modd defnyddio dysgu peirianyddol i ganfod rhai mathau o ymosodiadau seiber. Bydd yr ymchwil hwn yn parhau i wella ein dealltwriaeth o sut gallwn ddefnyddio deallusrwydd artiffisial i ganfod gweithgarwch maleisus.

[35] NCSC, Financial sector cyber collaboration centre (FSCCC) (2021)

Mae atal seiberdroseddau hefyd yn golygu mynd i'r afael â mathau eraill o weithgarwch troseddol

Mae seiberdroseddau (a ddiffinnir fel troseddau Deddf Camddefnyddio Cyfrifiaduron) yn digwydd pan fydd mynediad heb awdurdod at gyfrifiaduron, rhwydweithiau, data a dyfeisiau digidol eraill, gweithredoedd cysylltiedig sy'n achosi difrod neu greu neu gyflenwi offer i gyflawni'r troseddau hyn. Mae hyn yn gallu caniatáu i seiberdroseddwyr gyflawni rhagor o weithgareddau seiber maleisus fel ymosodiadau meddalwedd wystlo, mynediad heb awdurdod at gyfrifon, dwyn eiddo deallusol, ymosodiadau atal gwasanaeth, neu ddwyn setiau mawr o ddata personol – mae'r rhain yn droseddau sylweddol sydd ar gynnydd.

I ddinasyddion, mae seiberdroseddau'n aml yn dod i'r amlwg yn y troseddau pellach sy'n cael eu galluogi a'u hwyluso gan y seiberdroseddau. Gall mynediad heb awdurdod at gyfrifiadur arwain at amrywiaeth eang o dwyll, dwyn, blacmel rhywiol ac, mewn rhai achosion, hwyluso stelcio, cam-drin domestig ac aflonyddu. Mae pob un o'r troseddau hyn yn achosi niwed sylweddol i ddinasyddion y DU bob dydd, gan ddinistrio busnesau a difetha bywydau. Mae seiberdroseddau felly'n wahanol i faterion diogelwch ar-lein ehangach fel bwlio ac aflonyddu, iaith casineb, lledaenu twyllwybodaeth, hyrwyddo diwylliant gangiau a thrais, neu fynediad dan oed at bornograffi. Mae'r llywodraeth yn mynd i'r afael â'r materion hyn drwy'r papur gwyn ar niwed ar-lein a'r bil diogelwch ar-lein drafft.

Amcan 2: Atal ac amharu ar weithgarwch a gweithredwyr seiber troseddol, gwladwriaethol a maleisus eraill yn erbyn y DU, ei buddiannau a'i dinasyddion.

180. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

181. Mae'n fwy costus ac yn fwy o risg i weithredwyr seiber gwladwriaethol, troseddol a maleisus eraill dargedu'r DU. Byddwn yn cynnal ymgyrchoedd atal parhaus wedi'u teilwra sy'n defnyddio'r ystod lawn o alluoedd yn y DU (gan gynnwys ysgogiadau diplomyddol, economaidd, cudd a diplomyddol) i ddylanwadu ar ymddygiad gweithredwyr seiber maleisus a throseddol. Yn benodol, byddwn yn gwella ein signalau i'n gwrthwynebwyr o'n gallu a'n parodrwydd i osod costau ystyrlon, gan gynnwys drwy sancsiynau, asiantaethau gorfodi'r gyfraith a gweithrediadau'r NCF. A thrwy raglen Cyber Choices yr NCA, byddwn yn dargyfeirio unigolion rhag ymwneud â seiberdroseddu, gan weithio gyda diwydiant a'r byd academaidd i gynnig dewisiadau amgen gwell i ddarpar droseddwyr fel prentisiaethau a lleoliadau gwaith.

182. Byddwn hefyd yn darparu'r arfau a'r pwerau sydd eu hangen ar asiantaethau gorfodi'r gyfraith a'r asiantaethau cudd-wybodaeth drwy'r Bil Bygythiadau gan Wladwriaethau, drwy ddiweddaru'r ddeddfwriaeth bresennol a chyflwyno troseddau newydd i roi cyfrif am sut mae bygythiadau gan wladwriaethau wedi esblygu. A byddwn yn diwygio Deddf Elw Troseddau 2002 er mwyn manteisio i'r eithaf ar allu asiantaethau gorfodi'r gyfraith i ganfod, i atafaelu ac i adennill enillion seiberdroseddu. Yn benodol, byddwn yn gwneud hyn drwy greu pŵer fforffedu sifil i liniaru'r risgiau a berir gan y rheini na ellir eu herlyn.

183. Nid yw hi mor hawdd i weithredwyr seiber gwladwriaethol, troseddol a maleisus eraill dargedu'r DU oherwydd ein bod yn amharu ac yn difenwi eu gweithgareddau a'u galluoedd. Byddwn yn adolygu polisi a dull gweithredu'r llywodraeth ar gyfer mynd i'r afael â meddalwedd wystlo, gan fabwysiadu hyn fel un o'n hymgyrchoedd blaenoriaeth, gan gydweithio â'r diwydiant a'n partneriaid rhyngwladol. Byddwn yn manteisio i'r eithaf ar y partneriaethau rhwng yr NCF, yr NCSC, yr NCA ac asiantaethau gorfodi'r gyfraith yn ehangach a'r cymunedau diplomyddol a chudd-wybodaeth i wrthsefyll bygythiadau sy'n amharu ar gyfrinachedd, cywirdeb ac argaeledd seiberofod neu ddata a gwasanaethau mewn seiberofod. Yn benodol, byddwn yn buddsoddi mewn galluoedd i dargedu seilwaith seiberdroseddol a defnyddio ein gallu i orfodi'r gyfraith a'n galluoedd seiber ymosodol i amharu ar weithgareddau seiber maleisus. Mae ein gwrthwynebwyr yn meithrin galluoedd seiber ac yn eu defnyddio fwyfwy at ddibenion niweidiol. Byddwn yn defnyddio'r NCF yn llawn pan fyddwn yn credu bod hynny'n briodol, i amharu ar yr ymdrechion hyn ac amddiffyn a diogelu'r DU.

184. Byddwn hefyd yn gwrthsefyll y cynnydd mewn galluoedd seiber o ansawdd uchel i wladwriaethau a grwpiau troseddau cyfundrefnol drwy farchnadoedd masnachol a throseddol, gan fynd i'r afael â fforymau sy'n galluogi, yn hwyluso neu'n glamoreiddio seiberdroseddu.

185. Cynnydd mewn cyfiawnder troseddol a chanlyniadau aflonyddol eraill ar gyfer seiberdroseddwyr gyda gwell gallu o ran cyfiawnder troseddol yn cael ei ddefnyddio i erlyn seiberdroseddwyr yn y DU. Byddwn yn adolygu'r Ddeddf Camddefnyddio Cyfrifiaduron a phwerau perthnasol i sicrhau bod asiantaethau gorfodi'r gyfraith yn gallu ymchwilio i fygythiadau newydd a rhai sy'n dod i'r amlwg gan droseddwyr a chyflwyno erlynwyr mwy arbenigol i ddelio â'r nifer cynyddol o achosion seiber. Byddwn hefyd yn gwella sgiliau gorfodi'r gyfraith arbenigol, ymarfer a phrif ffrydio er mwyn sicrhau cyflenwad parhaus o swyddogion sydd â'r wybodaeth arbenigol seiber sydd ei hangen, drwy brosbectws sgiliau seiber Cyngor Cenedlaethol Prif Swyddogion yr Heddlu a Llwybrau Gyrfa Digidol y Coleg Plismona.

Susan Moody, Swyddog Atal Gwasanaeth Heddlu Gogledd Iwerddon (PSNI)

O'r chwith i'r dde Susan Moody (PSNI), Sarah Travers (Cyflwynydd Teledu) a Joe Dolan (Pennaeth Canolfan Seiberddiogelwch Gogledd Iwerddon)

Mae cyfrifiaduron a dyfeisiau symudol yn rhan o fywyd bob dydd pobl ifanc. Maen nhw'n cynnig cyfleoedd gwych ond maen nhw hefyd yn peri peryglon os ydyn nhw'n cael eu camddefnyddio. Mae'r swyddogaeth atal yng Ngwasanaeth Heddlu Gogledd Iwerddon yn camu mewn yn gynnar gyda phobl ifanc ac yn eu helpu i ddeall y gyfraith sy'n berthnasol i ddefnyddio a chamddefnyddio cyfrifiaduron. Mae hyn yn tynnu sylw at yr arwyddion o berygl sy'n gysylltiedig â gweithgarwch troseddol posibl ac mae hefyd yn tynnu sylw at y cyfleoedd gwych sydd ar gael drwy fentrau fel CyberFirst ac ystyried gyrfa yn y maes seiber, sy'n gallu rhoi dewis arall yn lle troseddu i'r rheini sydd â thalent neu chwilfrydedd, ac atal pobl eraill rhag eu camddefnyddio am resymau troseddol. Mae Susan wedi gweithio'n ddiflino i ddatblygu rhaglen gwybodaeth am seiberddiogelwch i ysgolion sydd ar gael i bob ysgol uwchradd ac mae wedi ymgysylltu'n uniongyrchol â mwy na 40 o ysgolion cynradd, nifer o ysgolion uwchradd, sefydliadau pobl ifanc a grwpiau mewn iwnifform. Gallai'r bobl ifanc hyn fod yn seiber lysgenhadon ac yn amddiffynwyr y dyfodol.

Amcan 3: Gweithredu mewn seiberofod a drwyddo i gefnogi ein diogelwch gwladol ac atal a chanfod troseddau difrifol

186. Byddwn yn cyflawni'r canlyniadau canlynol erbyn 2025:

187. Mae galluoedd seiber y DU yn cael mwy o effaith ar atal ac amharu ar fygythiadau nad ydynt yn rhai seiber. Byddwn yn uwchraddio ac yn datblygu'r NCF, gan gyflawni ein gweledigaeth hirdymor ar gyfer y gallu allweddol hwn, gan sicrhau ei fod wedi'i integreiddio'n llawn â Phencadlys Cyfathrebu Llywodraeth y DU, y Weinyddiaeth Amddiffyn, SIS a Dstl a gweithio'n agos gydag asiantaethau gorfodi'r gyfraith a llywodraeth ehangach. Byddwn yn cyflawni gweithrediadau seiber ymosodol cyfreithlon a chymesur drwy'r NCF, gan weithredu'n gyfrifol mewn seiberofod ac arwain drwy esiampl. Bydd gweithrediadau seiber ymosodol yn parhau i gefnogi diogelwch gwladol y DU, gan gynnwys ein polisi amddiffyn a thramor, ac atal troseddau difrifol.

188. Byddwn hefyd yn cynyddu ac yn datblygu galluoedd technegol asiantaethau gorfodi'r gyfraith yn erbyn seilwaith a chryptoarian, y gellir eu defnyddio yn erbyn bygythiadau eraill.

189. Mae galluoedd seiber y DU wedi'u hintegreiddio ar draws ystod lawn y gweithrediadau amddiffyn yn unol â'r Cysyniad Gweithredu Integredig 2025.[36] Bydd hyn yn cynnal ein mantais gystadleuol mewn rhyfel yn erbyn gwrthwynebwyr ac yn galluogi mwy o gydweithio â'n cynghreiriaid a'n partneriaid. Byddwn yn parhau i ddatblygu'r Rhaglen Newid Integreiddio Amddiffyn Aml-Barth, a fydd yn dod â galluoedd at ei gilydd ar draws y parthau, ac yn integreiddio'n well ag offerynnau eraill ein pŵer gwladol, gan gryfhau ein mantais filwrol dros ein gwrthwynebwyr. Bydd seiber yn rhan brif ffrwd o fusnes amddiffyn sy'n cael ei alluogi gan arbenigwyr seiber medrus iawn, ymwybyddiaeth seiber gyffredinol ar draws y gweithlu amddiffyn a galluoedd seiber blaengar a chadarn.

[36] Y Weinyddiaeth Amddiffyn, Integrated Operating Concept (2020)

Ymchwiliadau mawr i seiberdroseddau gan asiantaethau gorfodi'r gyfraith

Ymgyrch Imperil: Roedd yr Ymgyrch Imperil yn ymchwiliad ar y cyd rhwng Uned Troseddau Cyfundrefnol Ranbarthol De Ddwyrain Lloegr (SEROCU) a'r FBI i wefan a oedd yn gwerthu gwybodaeth bersonol a gwybodaeth bancio dioddefwyr ymosodiadau seiber. Roedd hyn yn golygu bod pobl eraill yn gallu prynu data personol i gyflawni twyll a throseddau eraill yn ymwneud â chamddefnyddio cyfrifiaduron. Roedd ymchwiliad mawr wedi arwain at adnabod cyfrifon banc a thaliadau a ddefnyddiwyd ar gyfer y seilwaith technegol, gan ganfod bod perchennog y wefan ym Mhacistan. Roedd hyn yn golygu bod yr FBI wedi gallu meddiannu'r wefan yn gudd ac wedyn ei thynnu i lawr. Arestiodd Uned Troseddau Cyfundrefnol Ranbarthol De Ddwyrain Lloegr y prif unigolyn a oedd dan amheuaeth a chanfuwyd ei fod wedi agor cyfrif banc yn yr Unol Daleithiau ar ran perchennog y wefan i wyngalchu arian troseddol. Roedd yr unigolyn dan amheuaeth yn y DU wedi cyflawni twyll sylweddol drwy ddefnyddio rhywfaint o'r data am y dioddefwyr, gan agor cyfrifon banc gydag enwau eraill, defnyddio cyfrifon banc pobl eraill i dalu am wyliau moethus a chyflwyno hawliadau ffug i'r Adran Gwaith a Phensiynau a oedd wedi golygu bod y wladwriaeth wedi colli dros £90,000. Cafodd yr unigolyn ei gyhuddo o naw cyhuddiad a chafodd ei ddedfrydu i bedair blynedd o garchar a oedd wedi'i leihau oherwydd ei fod wedi pledio'n euog yn gynnar. Rhoddodd y barnwr Gymeradwyaeth Barnwr i'r tîm ymchwilio. Adeg cyhoeddi mae cais yn mynd rhagddo am Atafaelu a Deddf Elw Troseddau gydol oes.

Ymgyrch Nipigon: Roedd hwn yn ymchwiliad gan Heddlu'r Met i un o ddinasyddion Bwlgaria yr oedd amheuaeth ei fod wedi creu tudalennau gwe-rwydo pwrpasol. Amcangyfrifwyd eu bod wedi achosi dros £40 miliwn o golledion ariannol i'r DU. Daethpwyd o hyd iddo ar ôl ymchwiliad i seiberdroseddwr adnabyddus arall a oedd wedi cael ei ddedfrydu i 10 mlynedd o garchar yn 2018, a oedd yn defnyddio'r tudalennau gwe-rwydo a gafodd eu creu gan yr unigolyn o Fwlgaria er mwyn cyflawni ei droseddau ei hun. Agorwyd yr ymchwiliad ar ôl canfod bod llawer iawn o gyfeiriadau e-bost yn gysylltiedig i'r unigolyn dan sylw. Ar ôl nifer o ymchwiliadau cymhleth a hir arweiniodd hynnny at gysylltu â'r awdurdodau ym Mwlgaria a chafodd yr unigolyn ei arestio, ei estraddodi ac ar ôl datgeliad cynhwysfawr, plediodd yn euog i bob cyhuddiad troseddol a derbyniodd dedfryd o garchar am naw mlynedd a hanner.

Ymgyrch Leasing: Yn 2020, arweiniodd yr NCA ymchwiliad i fygythiadau gan derfysgwyr i fomio'r GIG ar anterth pandemig COVID-19, gan fynnu taliadau mewn Bitcoin (BTC). Gan weithio gydag awdurdodau yn yr Almaen, daeth yr NCA o hyd i'r unigolyn dan amheuaeth ac fe'i cafwyd yn euog mewn llys yn yr Almaen.

Ar 12 Ebrill 2020, anfonodd un o ddinasyddion yr Eidal, a oedd yn byw yn yr Almaen, neges e-bost drwy'r rhwydwaith TOR yn dweud ei fod yn bwriadu bomio un o ysbytai'r GIG oni bai ei fod yn cael £10 miliwn mewn Bitcoin.

Cafodd hyn ei ddynodi'n gyflym fel blaenoriaeth uchel gan yr NCA a gofynnwyd i swyddogion seiberdroseddu arbenigol ddod o hyd i'r unigolyn a oedd yn gwneud hyn ac atal unrhyw ymosodiad posibl.

Roedd y drwgweithredwr hefyd wedi anfon negeseuon e-bost yn bygwth ymosod ar Aelodau Seneddol a bomio protestwyr Mae Bywydau Du o Bwys yn Llundain. Er ei fod wedi ysgrifennu ei negeseuon e-bost yn Saesneg, defnyddiodd ymchwilwyr yr NCA dechnegau seiber arbenigol a dadansoddiadau ymddygiadol ac ieithyddol i gasglu bod y troseddwr yn debygol o fod yn siaradwr Almaeneg brodorol.

Ar y cyd ag awdurdodau'r Almaen, gwelodd swyddogion yr NCA fod y negeseuon e-bost yn cael eu hanfon o gyfrifiadur mewn cyfeiriad ym Merlin. Drwy gydweithio rhyngwladol, ac er gwaethaf ymdrechion sylweddol i guddio ei hunaniaeth a'i leoliad, cafodd y drwgweithredwr ei adnabod a'i oruchwylio gan asiantaethau gorfodi'r gyfraith yn yr Almaen. Ar 15 Mehefin 2020, cafodd yr unigolyn ei arestio, ei gyhuddo o orfodaeth a chafodd ei remandio yn y ddalfa. Fe'i cafwyd yn euog ar 26 Chwefror 2021 a'i ddedfrydu i dair blynedd o garchar.

Cymryd camau drwy seiberofod i atal terfysgaeth

Ymgyrch yn Erbyn Daesh: Mae gwaith y Weinyddiaeth Amddiffyn a Phencadlys Cyfathrebu Llywodraeth y DU yn erbyn Daesh yn enghraifft o sut rydym wedi cymryd camau gweithredol i wrthsefyll bygythiadau gan y rheini sy'n camddefnyddio pŵer y rhyngrwyd a dulliau cyfathrebu modern.

Roedd Daesh wedi neilltuo llawer o amser ac egni i dechnoleg, i greu cynnwys ar y cyfryngau sy'n cael ei ddefnyddio i ddenu ac i radicaleiddio recriwtiaid newydd ac i ysbrydoli ymosodiadau terfysgol ar draws y byd. Dros y blynyddoedd diwethaf, rydym wedi gweld effaith y dull hwn ledled Ewrop, gan gynnwys ymosodiadau yn Llundain a Manceinion. Roedd Daesh hefyd wedi defnyddio systemau cyfathrebu modern i reoli eu gweithrediadau ym maes y gad. Roedd hyn yn caniatáu iddynt weithredu'n hyblyg, ar raddfa fawr ac yn gyflym, a pheri mwy fyth o berygl i'r poblogaethau roeddent yn ceisio eu rheoli, ac ymestyn eu cyrhaeddiad ar draws eu califfaeth fel y'i gelwir.

Yn ystod Brwydr Mosul, y ddinas roedd Daesh yn ei hystyried yn brifddinas iddynt, roeddem wedi defnyddio offer a thechnegau seiber mewn ymgyrchoedd ochr yn ochr â'r fyddin i gefnogi'r glymblaid ac fel rhan o ymgyrch sbectrwm llawn ehangach. Cafwyd amrywiaeth eang o ganlyniadau i'r gweithrediadau hyn. Roedd modd lleihau effeithiolrwydd Daesh drwy amharu ar gyfathrebu, diraddio propaganda, achosi diffyg ymddiriedaeth mewn grwpiau a gwadu offer a rhwydweithiau a oedd yn cael eu defnyddio fel rhan o'u hymgyrchoedd. Roeddem hefyd yn gallu defnyddio technegau seiber i hyrwyddo negeseuon llywodraeth y DU i dargedau, neu i dynnu sylw at eu gweithgareddau ymysg y rheini a allai fod yn eu helpu yn ddiarwybod. Roedd yr ymgyrchoedd hyn yn help mawr i ymdrechion y glymblaid i atal propaganda Daesh, yn llesteirio eu gallu i gydlynu ymosodiadau, ac roedd yn diogelu lluoedd y glymblaid ar faes y gad.

Andrew, aelod o'r Llu Seiber Cenedlaethol

Mae'r dechnoleg ddiweddaraf wastad wedi bod o ddiddordeb i mi. Cyn gweithio i'r gwasanaethau cudd-wybodaeth, fe wnes i ymuno â'r heddlu a gweithio fy ffordd i fyny o fod yn Gwnstabl i arbenigo mewn gwaith fforensig digidol – gan edrych ar ddyfeisiau electronig unigolion i gael tystiolaeth. Roeddwn i wrth fy modd ond roeddwn i eisiau gweld pa gyfleoedd eraill oedd ar gael.

Wnes i ddim mynd i'r brifysgol ar ôl gadael yr ysgol ac mae fy ngyrfa hyd yma wedi cael ei harwain gan chwilfrydedd naturiol, ac mae hynny'n wir am fy holl gydweithwyr sy'n ymuno â'r Llu Seiber Cenedlaethol. Maen nhw'n dod o bob math o gefndiroedd. Mae gennych arbenigwyr technegol dwfn wrth galon popeth, yn ogystal â chyn-reolwr archfarchnad, athro ysgol gynradd ac ymladdwr tân. Yr un peth sydd gan bob un ohonom yn gyffredin yw meddwl agored, dyhead i ddysgu a nod cyffredin o gadw'r wlad yn ddiogel – gan weld y bygythiadau a'r cyfleoedd ar gyfer diogelwch gwladol yn sgil technoleg newydd.

Fel heddwas, roeddwn i'n hynod falch o helpu pobl ar lefel bersonol. Heddiw, fel rhan o'r tîm unigryw hwn yn y Llu Seiber Cenedlaethol, rydw i'n helpu ar raddfa fyd-eang.

Cyflawni ein Huchelgais

190. Ni fydd y strategaeth hon yn golygu dim heb ddull trylwyr o weithredu ei hamcanion, monitro a gwerthuso cynnydd, a chael mecanweithiau i addasu pethau lle bo angen. Mae'r bennod hon yn nodi sut byddwn yn cyflawni hyn.

Rolau a chyfrifoldebau ar draws Llywodraeth

191. Bydd y Strategaeth Seiber Genedlaethol yn un o'r is-strategaethau a fydd, gyda'i gilydd, yn cyflawni uchelgeisiau'r Adolygiad Integredig. Bydd y Cyngor Diogelwch Gwladol yn goruchwylio'r strategaethau hyn gan Weinidogion, gan fonitro'r gweithredu ac ystyried cydbwysedd a chyfeiriad cyffredinol strategaeth y DU. Bydd cynnydd yn erbyn amcanion y strategaeth hefyd yn cael ei asesu drwy Fframwaith Cynllunio a Pherfformiad y Llywodraeth a'r Cynlluniau Cyflawni Canlyniadau.

192. Mae pob gweinidog yn chwarae rhan yn y gwaith o sicrhau bod y DU yn cadarnhau ei safle fel pŵer seiber cyfrifol a democrataidd, sy'n gallu diogelu a hyrwyddo ei buddiannau mewn seiberofod a thrwyddo. Mae'r rhestr hon yn cynnwys set benodol o gyfrifoldebau ar gyfer gweinidogion mewn rolau arweiniol, naill ai ar gyfer gweithredu neu gydlynu un neu ragor o bum elfen ein Strategaeth Seiber Genedlaethol neu ar gyfer goruchwylio ein penderfyniadau a'n galluoedd seiber pwysicaf.

- Mae **Canghellor Dugiaeth Caerhirfryn,** gyda chefnogaeth y **Tâl-feistr Cyffredinol**, yn darparu arweiniad cyffredinol ar draws adrannau i sicrhau ymateb effeithiol gan y llywodraeth i fygythiadau seiber, a chyflawni ein huchelgeisiau fel pŵer seiber. Mae hyn yn cynnwys datblygu a gweithredu'r Strategaeth Seiber Genedlaethol, y rhaglen gefnogi ar gyfer buddsoddi a chydlynu ymdrechion y llywodraeth ar seiberddiogelwch. Mae ganddynt hefyd gyfrifoldeb polisi a chydlynu traws-sector cyffredinol dros seiberddiogelwch a seibergadernid seilwaith cenedlaethol hanfodol y DU. Canghellor Dugiaeth Caerhirfryn yw'r cadeirydd diofyn ar

gyfer cyfarfodydd COBR gweinidogol ar ddigwyddiadau seiber, pan fydd eu hangen.

- Mae gan **Ysgrifennydd Gwladol yr Adran Gartref** rôl allweddol yn y gwaith o gyflawni'r Strategaeth Seiber Genedlaethol yn ei chyfanrwydd, ac yn yr ymateb i ddigwyddiadau seiber yn unol â'u cyfrifoldebau dros ddiogelwch y wlad. Mae'n arwain gwaith y llywodraeth i ganfod, atal a tharfu ar ein gwrthwynebwyr ochr yn ochr â'r Ysgrifennydd Gwladol dros Faterion Tramor, y Gymanwlad a Datblygu a'r Ysgrifennydd Gwladol dros Amddiffyn ac yn cydlynu'r gwaith hwnnw'n gyffredinol. Mae hefyd yn gyfrifol yn benodol am wrthsefyll seiberdroseddu.

- Mae gan yr **Ysgrifennydd Gwladol dros Faterion Tramor, y Gymanwlad a Datblygu** gyfrifoldeb statudol dros Bencadlys Cyfathrebu Llywodraeth y DU ac felly dros y Ganolfan Seiberddiogelwch Genedlaethol. Mae'n arwain gwaith y llywodraeth i ddatblygu arweinyddiaeth fyd-eang y DU ar faterion seiber ac mae'n gyfrifol yn benodol am y broses priodoli seiber, y drefn sancsiynau seiber ac ymgysylltu rhyngwladol ar gyfer digwyddiadau seiber categori uchel. Mae hefyd yn arwain gwaith y llywodraeth i ganfod, atal a tharfu ar ein gwrthwynebwyr ochr yn ochr â'r Ysgrifennydd Gwladol dros yr Adran Gartref a'r Ysgrifennydd Gwladol dros Amddiffyn.

- Mae'r **Ysgrifennydd Gwladol dros Amddiffyn** yn arwain gwaith y llywodraeth i ganfod, atal a tharfu ar ein gwrthwynebwyr ochr yn ochr â'r Ysgrifennydd Gwladol dros Faterion Tramor, y Gymanwlad a Datblygu a'r Ysgrifennydd Gwladol yr Adran Gartref.

- Mae'r **Ysgrifennydd Gwladol dros Faterion Tramor, y Gymanwlad a Datblygu a'r Ysgrifennydd Gwladol dros Amddiffyn** yn gyfrifol am y Llu Seiber Cenedlaethol, fel ymdrech ar y cyd rhwng amddiffyn a chudd-wybodaeth.

- Mae'r **Ysgrifennydd Gwladol dros Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon** yn arwain ar seiberddiogelwch sefydliadau yn yr economi ehangach gan ei fod yn ymwneud â pholisi digidol, a'r agweddau perthnasol ar dwf, arloesedd a sgiliau yn y Strategaeth Seiber Genedlaethol. Mae'n arwain gwaith y llywodraeth i gryfhau ecosystem seiber y DU a chymryd yr awenau o ran technolegau sy'n hanfodol i bŵer seiber.

- Mae gan **Weinidogion holl Brif Adrannau'r Llywodraeth ar gyfer seilwaith cenedlaethol hanfodol** gyfrifoldeb dros y polisi seiberddiogelwch a seibergadernid ar gyfer eu sectorau.

- Dylai **pob gweinidog** oruchwylio seiberddiogelwch eu hadrannau a rhoi mesurau lliniaru priodol ar waith. Pan fydd adran yn goruchwylio elfen o'r sector cyhoeddus neu breifat (er enghraifft DLUHC a llywodraeth leol neu DEFRA a'r cwmnïau dŵr) mae'n gyfrifol am y polisïau seiber a'r gweithgareddau sicrwydd sy'n ymwneud â'r sector hwnnw.

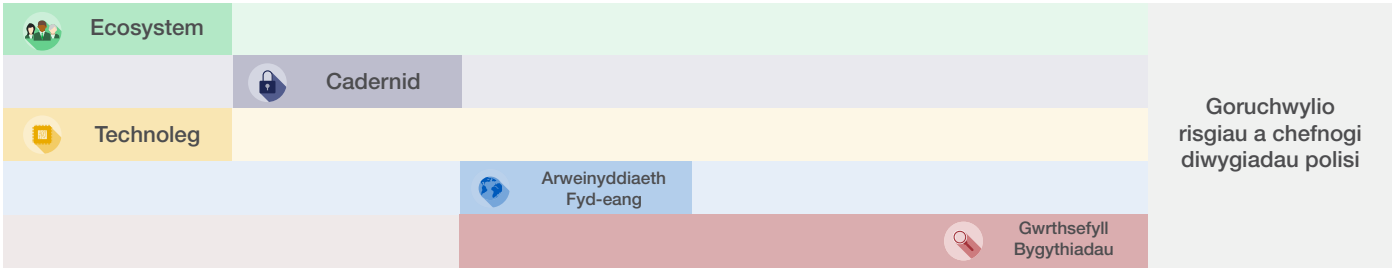
193. Y Dirprwy Gynghorydd Diogelwch Gwladol ar Gudd-wybodaeth, Diogelwch a Chadernid yw'r Uwch Berchennog Cyfrifol ar gyfer y strategaeth a bydd yn arwain y gwaith o gyflawni ar draws y llywodraeth ar lefel swyddogol, gyda chefnogaeth yr uwch swyddogion perthnasol ar draws adrannau.

Cyfrifoldebau Gweinidogol

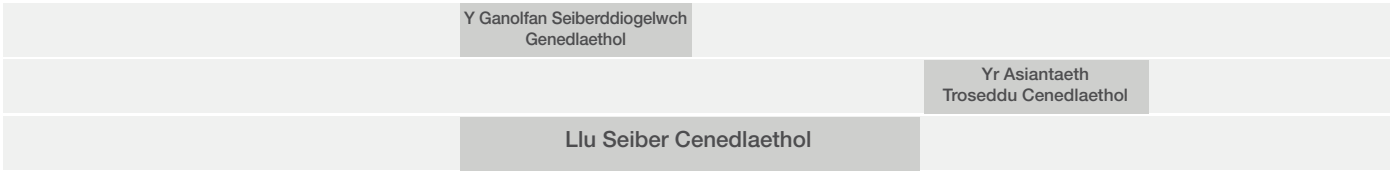
Prif Weinidog

Ysgrifennydd Digidol	Canghellor Dugiaeth Caerhirfryn*	Ysgrifennydd Tramor	Yr Ysgrifennydd Amddiffyn	Yr Ysgrifennydd Cartref	Pob Ysgrifennydd Gwladol

Cydlynu ac arwain y colofnau strategol



Cymorth cyflawni a gweithrediadau ar draws y strategaeth



*yn darparu arweiniad cyffredinol ar draws adrannau i sicrhau ymateb effeithiol gan y llywodraeth i fygythiadau seiber, a chyflawni ein huchelgeisiau fel pŵer seiber.

Buddsoddi yn ein pŵer seiber

194. Bydd y llywodraeth yn buddsoddi £2.6 biliwn mewn seiber a hen TG dros y tair blynedd nesaf. Mae hyn yn ychwanegol at fuddsoddiad sylweddol yn y Llu Seiber Cenedlaethol. Mae'n cynnwys cynnydd o £114 miliwn yn y Rhaglen Seiberddiogelwch Genedlaethol, gyda gwariant blynyddol ar allu wedi'i adeiladu o dan strategaeth 2016 yn cael ei symud o dan reolaeth adrannol ac yn cael ei roi ar sail barhaol. Bydd rhaglenni rhyngwladol yn cael eu darparu drwy'r Gronfa Gwrthdaro, Sefydlogrwydd a Diogelwch (CSSF) i helpu gwledydd sy'n bartneriaid i feithrin eu seibergadernid a gwrthsefyll bygythiadau seiber. Mae hyn ochr yn ochr â chynnydd mewn buddsoddiad a gyhoeddwyd hefyd mewn ymchwil a datblygu, cudd-wybodaeth, amddiffyn, arloesi, seilwaith a sgiliau, a bydd pob un ohonynt yn cyfrannu'n rhannol at bŵer seiber y DU.[37]

Mesur llwyddiant

195. Bydd y strategaeth yn cael ei llywodraethu gan fframwaith perfformiad sy'n esblygu'n barhaus ac sy'n adrodd i uwch swyddogion cyfrifol a'r Cyngor Diogelwch Gwladol. Bydd y fframwaith yn cael ei ddefnyddio fel sail i drafodaethau gyda'r senedd a chyrff eraill sy'n goruchwylio gwaith y gymuned diogelwch gwladol. Yn unol â dull gweithredu Strategaeth Seiberddiogelwch Genedlaethol 2016-2021, ni fydd yn ddogfen gyhoeddus oherwydd yr wybodaeth sensitif sydd ynddi, ond bydd y llywodraeth yn cyhoeddi adroddiadau cynnydd blynyddol.

196. Bydd y fframwaith perfformiad hwn yn:

- Darparu llwybr clir o sut bydd gweithgareddau yn arwain at yr amrywiol amcanion a amlinellir yn y strategaeth
- Sicrhau atebolrwydd dros gyflwyno'r strategaeth
- Darparu tryloywder ynghylch y cynnydd y mae'r wlad yn ei wneud at nodau'r strategaeth
- Dangos sut mae angen addasu gweithgarwch er mwyn sicrhau ei fod yn cyd-fynd â'r strategaeth
- Deall pa weithgareddau sy'n llwyddo i gyflawni uchelgeisiau strategol, er mwyn gallu defnyddio'r gwersi hyn yn y dyfodol
- Darparu darlun cyfannol o weithgarwch ar draws y pum colofn, gan leihau dyblygu a nodi cryfderau a gwendidau ym mhŵer seiber y wlad
- Sicrhau bod y strategaeth yn darparu cymorth seiber i bob rhan o gymdeithas

[37] Trysorlys Ei Mawrhydi, Autumn Budget and Spending Review 2021 (2021)

Y camau nesaf

197. Bwriedir i'r strategaeth hon fod yn ganllaw i weithredu, nid yn unig ar gyfer y rheini mewn llywodraeth sy'n gyfrifol am seiber a'r ystod eang o bolisïau cysylltiedig eraill (gweler Atodiad A) ond hefyd ar gyfer pob unigolyn a sefydliad ar draws ein cymdeithas gyfan sydd â diddordeb a chyfrifoldeb dros ein hymdrech seiber genedlaethol. Mae hefyd yn ddechrau sgwrs mae arnom eisiau ei pharhau, i sicrhau bod ein hamcanion a'n blaenoriaethau'n dal yn berthnasol dros y pump i ddeng mlynedd nesaf. Bydd cyhoeddi'r strategaeth hon yn blatfform i ymgysylltu rhagor â'r sector cyhoeddus, y sector preifat a'r trydydd sector ar draws y DU ac rydym yn gofyn am adborth uniongyrchol i ukcyberstrategy@cabinetoffice.gov.uk. Byddwn yn adrodd yn ôl yn flynyddol ar y cynnydd rydym yn ei wneud i roi'r strategaeth hon ar waith.

Atodiad A: Seiber fel rhan o agenda ehangach y llywodraeth

Bwriad y Strategaeth Seiber Genedlaethol yw cefnogi a datblygu amrywiaeth o flaenoriaethau eraill ar gyfer y Llywodraeth ym maes diogelwch, amddiffyn, polisi tramor a'n hagenda economaidd. Yn ei thro, bydd y strategaeth hon yn dibynnu ar y galluoedd ehangach a ddatblygwyd drwy ein system addysg a sgiliau a'n dull gweithredu cenedlaethol o ran polisi diwydiannol digidol a thechnoleg, ymchwil a thwf busnes. Dyma rai o'r prif strategaethau a chynlluniau perthnasol:

- **Yr Adolygiad Integredig**, gan gynnwys ymdrechion cenedlaethol i wella cadernid, mynd i'r afael â bygythiadau i'r wladwriaeth, troseddu cyfundrefnol difrifol a therfysgaeth, cynnal ein mantais strategol drwy wyddoniaeth a thechnoleg, a siapio'r drefn ryngwladol
- Mae'r **Strategaeth Ddata Genedlaethol** yn nodi ein gweledigaeth i harneisio pŵer defnyddio data yn gyfrifol i roi hwb i gynhyrchiant, creu busnesau a swyddi newydd, gwella gwasanaethau cyhoeddus, cefnogi cymdeithas decach, a sbarduno darganfyddiadau gwyddonol, gan roi'r DU ar flaen y gad y don nesaf o arloesi. Mae hyn yn cynnwys trawsnewid defnydd y llywodraeth o ddata er mwyn gwella effeithlonrwydd a gwella gwasanaethau cyhoeddus drwy fynd i'r afael â'r rhwystrau i rannu data rhwng adrannau a gwella ansawdd y data sydd ganddynt. Bydd hyn yn hanfodol i gefnogi ein hagenda seiber drwy sicrhau ein bod yn gallu casglu a defnyddio data o ansawdd da am ddigwyddiadau seiber
- **Y cynllun ar gyfer twf,** sy'n ein helpu i **Ailgodi'n Gryfach** drwy gymorth a buddsoddiad ychwanegol ar gyfer seilwaith, sgiliau ac arloesedd, a'r **Strategaeth Arloesi** sy'n gosod ein dyheadau ar gyfer economi sy'n cael ei harwain gan arloesedd
- **Y Cynllun ar gyfer Rheoleiddio Digidol**, sy'n nodi ein dull rhagweithiol o reoleiddio technolegau digidol mewn ffordd sy'n ysgogi ffyniant ac yn meithrin ymddiriedaeth yn eu defnydd
- **Y Strategaeth Deallusrwydd Artiffisial Genedlaethol**, sy'n ceisio paratoi'r DU ar gyfer y degawd trawsnewidiol nesaf mewn AI drwy fuddsoddi yn anghenion hirdymor yr ecosystem AI, cefnogi'r broses o drawsnewid i economi sy'n manteisio ar AI, a sicrhau bod y DU yn llywodraethu technolegau AI yn gywir yn genedlaethol ac yn rhyngwladol. Mae hyn hefyd yn cynnwys mesurau i gefnogi arloesedd seiberddiogelwch mewn systemau a alluogir gan AI ar yr un pryd â diogelu'r cyhoedd a meithrin ymddiriedaeth yn ei ddefnydd
- Bydd y **Strategaeth Cadernid Genedlaethol**, sydd ar y gweill yn rhoi rhywfaint o sylw i sut bydd y DU yn aros ar flaen y gad o ran bygythiadau technolegol ac yn aros yn gadarn yn y seiberofod
- Bydd y **Strategaeth Ddigidol** sydd ar y gweill yn gosod gweledigaeth glir o uchelgais y llywodraeth i harneisio awydd newydd am drawsnewid digidol, sbarduno twf, a pharhau i adeiladu economi ddigidol fwy cynhwysol, cystadleuol ac arloesol ar gyfer y dyfodol; a fydd yn adeiladu ar Ddeg Blaenoriaeth Technoleg yr Adran dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon (DCMS) i fanylu ymhellach ar uchelgeisiau'r llywodraeth yn y sector digidol
- **Y Strategaeth Sero Net** i sicrhau bod ein heconomi ffyniannus sy'n cael ei harwain gan arloesedd yn un carbon isel
- **Y Cynllun Gorchfygu Troseddu**, sy'n nodi sut y byddwn yn adfer hyder yn y system cyfiawnder troseddol ac yn gwireddu ein gweledigaeth gyffredin o gael Prydain fwy diogel gyda llai o droseddu a llai o ddioddefwyr[38]

[38] Y Swyddfa Gartref, Y Cynllun Gorchfygu Troseddu (2021)

Wrth gefn y Strategaeth Seiber Genedlaethol mae dau gyhoeddiad arall sy'n nodi sut y bydd rhannau unigol o'r strategaeth yn cael eu cyflawni.

- Bydd **Strategaeth Seiberddiogelwch y Llywodraeth** sydd ar y gweill yn manylu ar y cynlluniau ar gyfer gwella diogelwch y llywodraeth a'r sector cyhoeddus, gan gefnogi'r strategaeth genedlaethol hon
- Bydd **Adolygiad o Gymhellion a Rheoliadau 2021** sydd ar y gweill yn nodi ein canfyddiadau ynghylch pa mor effeithiol mae ein gwaith o gymell gwelliannau mewn seiberddiogelwch yn yr economi ehangach wedi bod, a sut rydym yn bwriadu rhoi ar waith elfennau busnes a sefydliadol y golofn cadernid

Atodiad B: Rheoliadau NIS – Strategaeth Genedlaethol

Cyflwyniad

Strategaeth Genedlaethol NIS

1. Y Strategaeth Seiber Genedlaethol yw strategaeth genedlaethol y DU at ddibenion Rheoliad 2 o Reoliadau Rhwydweithiau a Systemau Gwybodaeth (NIS) y DU 2018.

2. Mae'r atodiad hwn yn rhoi rhagor o wybodaeth gan gynnwys:

- rolau a chyfrifoldebau'r awdurdodau allweddol sy'n gyfrifol am weithredu NIS yn y DU; a
- rhestr o'r awdurdodau allweddol perthnasol.

Rheoliadau NIS y DU

3. Yn 2016, cytunodd y Comisiwn Ewropeaidd ar Gyfarwyddeb gyda'r nod o gynyddu diogelwch Systemau Rhwydwaith a Gwybodaeth yn yr Undeb Ewropeaidd (UE). Cefnogwyd hyn gan Lywodraeth y DU.

4. Ar 20 Ebrill 2018, cyflwynodd y Llywodraeth gyfres newydd o reoliadau, sef Rheoliadau Rhwydweithiau a Systemau Gwybodaeth 2018 gerbron y Senedd. Daeth y Rheoliadau hyn i rym ar 10 Mai 2018.

5. Sefydlodd y Rheoliadau NIS drefn reoleiddio newydd yn y DU sy'n mynnu bod gweithredwyr dynodedig gwasanaethau hanfodol a darparwyr gwasanaethau digidol perthnasol yn rhoi mesurau technegol a sefydliadol ar waith i ddiogelu eu rhwydwaith a'u systemau gwybodaeth.

6. Mae'n berthnasol i sectorau sy'n hanfodol i'n heconomi a'n cymdeithas ac sy'n dibynnu'n drwm ar systemau gwybodaeth a rhwydweithiau; megis ynni, trafnidiaeth, dŵr yfed, gofal iechyd a seilwaith digidol.

7. Mae darparwyr gwasanaethau digidol allweddol (megis peiriannau chwilio, gwasanaethau cyfrifiadura yn y cwmwl a marchnadoedd ar-lein) hefyd wedi'u cynnwys.

8. Mae'r Rheoliadau NIS yn sefydlu:

- **fframwaith cenedlaethol** i gefnogi'r gweithredu, gan gynnwys strategaeth genedlaethol;
- **awdurdodau cymwys** sy'n benodol i sectorau yn gweithredu fel rheoleiddwyr;
- y Ganolfan Seiberddiogelwch Genedlaethol (NCSC) fel **Un Pwynt Cyswllt** a'r **Tîm Ymateb i Ddigwyddiadau Diogelwch Cyfrifiadurol** (CSIRT).

9. Asesir cynnydd drwy gynnal Adolygiadau Ôl-weithredu bob 2-5 mlynedd.

Prif rolau a chyfrifoldebau

Y Fframwaith Cenedlaethol

10. Swyddfa'r Cabinet sy'n gyfrifol am y Strategaeth Seiber Genedlaethol, ac mae'r Strategaeth Genedlaethol NIS yn rhan o hynny. Mae gan Swyddfa'r Cabinet hefyd gyfrifoldeb cyffredinol dros wella diogelwch a chadernid seilweithiau cenedlaethol hanfodol.

11. Yr Adran dros Dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon (DCMS) sy'n gyfrifol am weithredu'r Rheoliadau NIS yn gyffredinol, gan gynnwys cydlynu'r awdurdodau perthnasol a'r NCSC. Mae'r Adran dros Dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon yn cyhoeddi canllawiau i awdurdodau cymwys er mwyn cefnogi'r gwaith ehangach o roi'r NIS ar waith ledled y DU.

Un Pwynt Cyswllt

12. Y pwynt cyswllt cenedlaethol ar gyfer ymgysylltu â phartneriaid rhyngwladol [yr Undeb Ewropeaidd] ar NIS, cydlynu ceisiadau am weithredu neu am wybodaeth, a chyflwyno ystadegau blynyddol am ddigwyddiadau. Y Ganolfan Seiberddiogelwch Genedlaethol yw Un Pwynt Cyswllt y DU.

Tîm Ymateb i Ddigwyddiadau Diogelwch Cyfrifiadurol (CSIRT)

13. Y Ganolfan Seiberddiogelwch Genedlaethol yw CSIRT y DU. Mae'n gyfrifol am fonitro digwyddiadau seiberddiogelwch ar lefel genedlaethol; darparu dadansoddiad amser-real o fygythiadau, amddiffyn rhag ymosodiadau seiber cenedlaethol, darparu cyngor technegol, ac ymateb i ddigwyddiadau seiber mawr i helpu i leihau niwed.

14. Mae'r Ganolfan yn cynnal y Fframwaith Asesu Seiber seiliedig ar ganlyniadau ac yn darparu canllawiau helaeth ar faterion seiberddiogelwch fel yr Awdurdod Technegol Cenedlaethol.

Awdurdodau Cymwys

15. Mae'r rhain yn gyfrifol am oruchwylio a gorfodi Rheoliadau NIS yn eu sectorau, gan ddynodi ac asesu i ba raddau mae gweithredwyr gwasanaethau hanfodol a darparwyr gwasanaethau digidol perthnasol yn cydymffurfio â gofynion Rheoliadau NIS. Nodir y rhain yn Atodlen 1 Rheoliadau NIS ac mae rhestr yn adran 3.

Gweithredwyr Gwasanaethau Hanfodol a Darparwyr Gwasanaethau Digidol Perthnasol

16. Rhaid i'r Gweithredwyr a'r Darparwyr hyn sy'n croesi trothwyon dynodi y sector hwnnw, neu sydd wedi cael eu dynodi gan yr awdurdod perthnasol o dan Reoliad 8(3) o Reoliadau NIS, gydymffurfio â gofynion Rheoliadau NIS.

17. Mae'r rhain yn cynnwys:

- cymryd mesurau technegol a sefydliadol priodol a chymesur i reoli'r risgiau i ddiogelwch y rhwydwaith a'r systemau gwybodaeth;
- cymryd camau priodol a chymesur i atal a lleihau dylanwad digwyddiadau sy'n effeithio ar ddiogelwch y rhwydwaith a'r systemau gwybodaeth;
- hysbysu'r awdurdod cymwys perthnasol am unrhyw ddigwyddiad sy'n cael effaith sylweddol ar ei wasanaethau;
- bodloni'r gofynion arolygu o dan Reoliadau NIS; a
- cydymffurfio â hysbysiadau gwybodaeth, gorfodi a chosb.
- Mae'n rhaid i Ddarparwyr Gwasanaethau Digidol Perthnasol hefyd gofrestru gyda Swyddfa'r Comisiynydd Gwybodaeth.

Awdurdodau perthnasol eraill:

18. Mae Llywodraeth y DU yn gweithio'n agos gyda'r Gweinyddiaethau Datganoledig ac awdurdodau perthnasol eraill, gan gynnwys Adrannau Arweiniol y Llywodraeth, ar weithredu Rheoliadau NIS.

19. Mae'r Ganolfan Diogelu Seilwaith Cenedlaethol (CPNI) yn rhoi cyngor ar ddiogelwch personél a ffisegol cysylltiedig.

Rhestr o'r awdurdodau allweddol ar gyfer gweithredu NIS

Awdurdodau Cenedlaethol	
Rheoliadau NIS y DU	Yr Adran dros Dechnoleg Ddigidol, Diwylliant, y Cyfryngau a Chwaraeon
Strategaeth Seiber Genedlaethol y DU	Swyddfa'r Cabinet
Un Pwynt Cyswllt y DU	Y Ganolfan Seiberddiogelwch Genedlaethol
Tîm Ymateb i Ddigwyddiadau Diogelwch Cyfrifiadurol y DU (CSIRT)	Y Ganolfan Seiberddiogelwch Genedlaethol

Awdurdodau Cymwys					
Sector	**Is-sector**	**Lloegr**	**Cymru**	**Yr Alban**	**Gogledd Iwerddon**
Ynni	Trydan	Ar y cyd: Yr Adran Busnes, Ynni a Strategaeth Ddiwydiannol a'r Awdurdod Marchnadoedd Nwy a Thrydan (Ofgem)			Yr Adran Gyllid
	Olew	Yr Adran Busnes, Ynni a Strategaeth Ddiwydiannol			Yr Adran Gyllid
	Nwy	Ar y cyd: Yr Adran Busnes, Ynni a Strategaeth Ddiwydiannol a'r Awdurdod Marchnadoedd Nwy a Thrydan (Ofgem)[39]			Yr Adran Gyllid
Trafnidiaeth	Awyr	Ar y cyd: Yr Adran Drafnidiaeth a'r Awdurdod Hedfan Sifil (CAA)			
	Trên	Yr Adran Drafnidiaeth			Yr Adran Gyllid
	Dŵr	Yr Adran Drafnidiaeth			
	Ffordd	Yr Adran Drafnidiaeth		Gweinidogion yr Alban	Yr Adran Gyllid
Gofal iechyd	Lleoliadau gofal iechyd	Yr Adran Iechyd a Gofal Cymdeithasol	Gweinidogion Cymru	Gweinidogion yr Alban	Yr Adran Gyllid
Dŵr Yfed	Dŵr Yfed	Adran yr Amgylchedd, Bwyd a Materion Gwledig	Gweinidogion Cymru	Rheoleiddiwr Ansawdd Dŵr Yfed yr Alban	Yr Adran Gyllid
Seilwaith Digidol	Seilwaith Digidol	Y Swyddfa Gyfathrebiadau (Ofcom)			

[39] Ar gyfer rhai eithriadau, yr Adran Busnes, Ynni a Strategaeth Ddiwydiannol yw'r unig Awdurdod Cymwys. Ceir rhagor o fanylion yn Atodlen 1 a 2 Rheoliadau Rhwydweithiau a Systemau Gwybodaeth 2018.

Atodiad C: Geirfa

Action Fraud – canolfan riportio ar gyfer twyll a seiberdroseddu lle gall dinasyddion a sefydliadau gysylltu i riportio twyll os ydynt wedi cael eu twyllo neu wedi profi seiberdroseddu yng Nghymru, Lloegr a Gogledd Iwerddon. Yn yr Alban, caiff y rhain eu cyfeirio at Heddlu'r Alban.

Active Cyber Defence (ACD) – yn helpu sefydliadau i ddod o hyd i wendidau a'u datrys, rheoli digwyddiadau neu darfu'n awtomataidd ar ymosodiadau seiber. Mae rhai gwasanaethau wedi'u bwriadu ar gyfer y sector cyhoeddus yn bennaf, ac mae eraill ar gael yn fwy eang i'r sector preifat neu ddinasyddion, yn ôl y graddau y maent yn gymwys neu'n ddichonol.

Adolygiad Integredig – mae 'Global Britain in a Competitive Age, the Integrated Review of Security, Defence, Development and From Policy', yn disgrifio gweledigaeth y llywodraeth ar gyfer rôl y DU yn y byd dros y degawd nesaf a'r camau y bydd y llywodraeth yn eu cymryd hyd at 2025.

Awdurdodau Cymwys – cyrff rheoleiddio fel y'u disgrifir yn Rheoliadau Rhwydweithiau a Systemau Gwybodaeth (NIS) 2018. Mae nifer o awdurdodau cymwys yn gyfrifol am wahanol sectorau sy'n cael eu cwmpasu gan NIS.

Bygythiad seiber – unrhyw beth sy'n gallu peryglu diogelwch systemau gwybodaeth a dyfeisiau sydd wedi'u cysylltu â'r rhyngrwyd, neu achosi niwed iddynt (gan gynnwys caledwedd, meddalwedd a seilwaith cysylltiedig), y data sydd arnynt a'r gwasanaethau maen nhw'n eu darparu, yn bennaf drwy ddulliau seiber.

Canolfan Cydlynu Seiber y Llywodraeth (GCCC) – Menter arfaethedig ar y cyd rhwng GSG, CDDO a NCSC sy'n dod â'u priod swyddogaethau a meysydd arbenigedd at ei gilydd i gydlynu ymdrechion seiberddiogelwch gweithredol yn well ar draws y llywodraeth, trawsnewid sut mae data seiberddiogelwch a chudd-wybodaeth bygythiadau yn cael eu defnyddio ar draws y llywodraeth, a gwella gallu'r llywodraeth i 'amddiffyn fel un'.

COBR – Ystafell Friffio Swyddfa'r Cabinet. Mae ymateb llywodraeth ganolog y DU i argyfyngau yn seiliedig ar brosesau COBR; dyma'r lleoliad ffisegol, fel arfer yn San Steffan, lle mae'r ymateb canolog yn cael ei weithredu, ei fonitro a'i gydlynu ac mae'n ganolbwynt i ymateb y llywodraeth a ffynhonnell awdurdodol o gyngor i ymatebwyr lleol.

Corff Gwybodaeth Diogelwch Seiber (CyBOK) – Adnodd unigryw sy'n darparu, am y tro cyntaf, sylfaen o wybodaeth sy'n cwmpasu ehangder a dyfnder seiberddiogelwch, gan ddangos bod seiberddiogelwch yn cwmpasu ystod eang o ddisgyblaethau.

Crypt-Allwedd (CK) – y term sy'n cael ei ddefnyddio i ddisgrifio sut mae'r DU yn defnyddio cryptograffeg i ddiogelu'r wybodaeth a'r gwasanaethau hanfodol y mae cymuned diogelwch genedlaethol a milwrol y DU yn dibynnu arnynt, gan gynnwys rhag ymosodiad gan ein gwrthwynebwyr mwyaf galluog.

Cryptoarian – math o arian digidol a system dalu, e.e. Bitcoin.

Cryptograffeg – y wyddoniaeth neu'r astudiaeth sy'n dadansoddi a dehongli codau a seifferau; crypto-ddadansoddi.

Cynllun ar gyfer Rheoleiddio Digidol – mae'n nodi dull gweithredu cyffredinol y llywodraeth ar gyfer rheoli technolegau digidol er mwyn sbarduno twf ac arloesedd.

Darparwyr Gwasanaeth a Reolir – trydydd partïon sy'n darparu set o wasanaethau diffiniedig i gwsmer ac sy'n ysgwyddo'r cyfrifoldeb dros redeg, cynnal a sicrhau'r gwasanaethau hynny.

Deallusrwydd Artiffisial (AI) – technoleg lle mae system gyfrifiadurol yn cael ei chodio "i feddwl dros ei hun", gan addasu a gweithredu'n annibynnol. Gwneir defnydd cynyddol o AI ar gyfer tasgau mwy cymhleth, fel diagnosis meddygol, darganfod cyffuriau, a gwaith cynnal prosesau rhagfynegi.

Digwyddiad seiber – digwyddiad a all fod neu sydd yn fygythiad i gyfrifiadur, dyfais sydd wedi'i chysylltu â'r rhyngrwyd, neu rwydwaith – neu ddata sy'n cael ei brosesu, ei storio, neu ei drosglwyddo ar y systemau hynny – a lle bydd efallai angen ymateb i liniaru'r canlyniadau.

Dilysu – proses o wirio hunaniaeth neu briodoleddau eraill defnyddiwr, proses neu ddyfais.

Diogel drwy Ddylunio – meddalwedd, caledwedd a systemau sydd wedi cael eu dylunio o'r cychwyn i fod yn ddiogel.

Ecosystem seiber – yr holl seilwaith, unigolion, prosesau, data, gwybodaeth a thechnolegau cyfathrebu sy'n gysylltiedig â'i gilydd, ynghyd â'r amgylchedd a'r amodau sy'n dylanwadu ar y rhyngweithio hynny.

Fframwaith Asesu Seiber (CAF) – mae'n darparu dull systematig a chynhwysfawr o asesu'r graddau y mae risgiau seiber i swyddogaethau hanfodol yn cael eu rheoli gan y sefydliad cyfrifol.

Five Eyes – enw'r gynghrair gudd-wybodaeth rhwng UDA, y DU, Canada, Awstralia a Seland Newydd sy'n helpu i rannu gwybodaeth er mwyn cadw ei dinasyddion mor ddiogel â phosibl rhag bygythiadau.

Gefaill digidol – replica rhithiol neu gynrychiolaeth o asedau, prosesau, systemau neu sefydliadau yn yr amgylcheddau adeiledig, cymdeithasol neu naturiol sy'n rhoi cipolwg ar sut mae asedau ffisegol cymhleth a dinasyddion yn ymddwyn, gan helpu sefydliadau i wella'r broses o wneud penderfyniadau a gwneud y gorau o brosesau. Mae newidiadau yn y byd go iawn yn cael eu hadlewyrchu yn y gefaill digidol, a gellir dyblygu newidiadau yn y gefaill digidol yn awtomatig yn y byd go iawn.

GFCE – Fforwm Byd-eang ar Arbenigedd Seiber.

Gwasanaeth Riportio Gwendidau – mecanwaith y gellir ei ddefnyddio i hysbysu sefydliad am ddiffygion diogelwch cyn iddynt gael eu hecsbloetio gan ymosodwyr.

Gweithredwyr Gwasanaethau Hanfodol – sefydliadau mewn sectorau hanfodol sy'n dibynnu'n drwm ar rwydweithiau gwybodaeth, er enghraifft cyfleustodau, gofal iechyd, trafnidiaeth a seilwaith digidol fel y nodir yn y meini prawf yn Rheoliadau Rhwydweithiau a Systemau Gwybodaeth (NIS) 2018.

Gwendidau – chwilod mewn rhaglenni meddalwedd sydd â'r potensial i gael eu hecsbloetio gan ymosodwyr.

Hen TG – Mae hen TG yn cyfeirio at systemau sydd â chaledwedd a meddalwedd lle mae'r gwasanaethau cymorth gan y gwerthwr, y cymorth estynedig a/neu'r trefniadau cymorth penodol wedi dod i ben.

ICANN – Corfforaeth y Rhyngrwyd ar gyfer Enwau a Rhifau a Neilltuir. Mae'n cydlynu enwau gwefannau a chyfeiriadau IP.

Lleoedd Cysylltiedig – cymuned sy'n integreiddio technolegau gwybodaeth a chyfathrebu a dyfeisiau y Rhyngrwyd Pethau (IoT) i gasglu a dadansoddi data er mwyn darparu gwasanaethau newydd i'r amgylchedd adeiledig, a gwella ansawdd bywyd i ddinasyddion.

Llywodraeth ddatganoledig neu weinyddiaeth ddatganoledig – Y deddfwrfeydd a'r gweithrediaethau ar wahân yng Nghymru, yr Alban a Gogledd Iwerddon ar ôl datganoli, sy'n gyfrifol am lawer o faterion polisi domestig gyda'r pŵer i lunio deddfau yn y meysydd hyn.

Meddalwedd wystlo – meddalwedd maleisus sy'n rhwystro'r defnyddiwr rhag cael mynediad i'w ffeiliau, ei gyfrifiadur neu ei ddyfais nes bydd yn talu pridwerth.

Microgynhyrchu – cynhyrchu ynni ar raddfa fach gan gartrefi, busnesau bach a chymunedau.

NATO – Sefydliad Cytundeb Gogledd Iwerydd.

NCA – Yr Asiantaeth Troseddu Cenedlaethol.

OECD – Y Sefydliad ar gyfer Cydweithrediad a Datblygiad Economaidd. Sefydliad economaidd rhynglywodraethol.

Parth – mae enw parth yn dangos lleoliad sefydliad neu endid arall ar y rhyngrwyd ac mae'n cyfateb i gyfeiriad Protocol Rhyngrwyd (IP).

Pencadlys Cyfathrebu'r Llywodraeth (GCHQ) – y ganolfan ar gyfer gweithgareddau casglu cudd-wybodaeth signalau'r Llywodraeth a chartref yr Awdurdod Technegol Cenedlaethol ar gyfer Seiber (NTA).

Rheoliadau Rhwydweithiau a Systemau Gwybodaeth (NIS) 2018 – rheoliadau'r DU sy'n darparu mesurau cyfreithiol i roi hwb i ddiogelwch (cadernid ffisegol a seiber) systemau rhwydwaith a gwybodaeth ar gyfer darparu gwasanaethau hanfodol a gwasanaethau digidol.

Rheoli Digwyddiadau – rheoli a chydlynu gweithgareddau i ymchwilio ac adfer sgil-effeithiau gwirioneddol neu bosibl o ddigwyddiad seiber niweidiol a allai beryglu neu achosi niwed i system neu rwydwaith.

Rhyngrwyd – rhwydwaith cyfrifiadurol byd-eang, sy'n darparu amrywiaeth o gyfleusterau gwybodaeth a chyfathrebu, yn cynnwys rhwydweithiau rhyng-gysylltiedig gan ddefnyddio protocolau cyfathrebu safonol.

Risg seiber – posibilrwydd y bydd bygythiad seiber penodol yn ecsbloetio gwendidau system wybodaeth ac yn achosi niwed.

Seiberddiogelwch – diogelu systemau sydd wedi'u cysylltu â'r rhyngrwyd (gan gynnwys caledwedd, meddalwedd a seilwaith cysylltiedig), y data sydd arnynt, a'r gwasanaethau maent yn eu darparu, rhag mynediad heb awdurdod, niwed neu gamddefnydd. Mae hyn yn cynnwys niwed a achosir yn fwriadol gan weithredwr y system, neu'n ddamweiniol o ganlyniad i fethu â dilyn gweithdrefnau diogelwch neu gael ei gamarwain i wneud hynny.

Seiberdroseddau – troseddau sy'n seiliedig ar seiber (y gellir eu cyflawni dim ond drwy ddefnyddio dyfeisiau TGCh, lle mae dyfeisiau technolegol yn gyfrwng ar gyfer cyflawni'r trosedd yn ogystal â'r targed hefyd); neu droseddau sy'n cael eu galluogi ar sail seiber (troseddau y gellir eu cyflawni heb ddyfeisiau TGCh, fel twyll ariannol, ond sy'n gallu ehangu'n sylweddol o ran difrifoldeb a chyrhaeddiad drwy ddefnyddio TGCh).

Seibergadernid – gallu cyffredinol systemau, sefydliadau a dinasyddion i wrthsefyll digwyddiadau seiber a, lle mae niwed yn cael ei achosi, ymadfer ohonynt.

Seiber ymosodol – ychwanegu, dileu neu gamddefnyddio data ar systemau neu rwydweithiau i gael effaith gorfforol, rithwir neu wybyddol. Yn aml bydd gweithrediadau seiber ymosodol yn camfanteisio ar wendidau technegol, yn defnyddio systemau neu rwydweithiau mewn ffyrdd na fyddai eu perchnogion a'u gweithredwyr yn eu bwriadu neu'n eu cymeradwyo, ac maent yn aml yn ddibynnol ar dwyll neu gamgynrychiolaeth.

Seilwaith Cenedlaethol Hanfodol – Yr elfennau hanfodol hynny o seilwaith (sef asedau, cyfleusterau, systemau, rhwydweithiau neu brosesau a'r gweithwyr hanfodol sy'n eu gweithredu a'u hwyluso), a allai arwain at y canlynol:

a. effaith negyddol ddifrifol ar argaeledd, cywirdeb neu gyflenwad gwasanaethau hanfodol – gan gynnwys y gwasanaethau hynny, os ydynt yn cael eu peryglu, a all arwain at bobl yn cael eu hanafu neu eu lladd ar raddfa fawr – gan ystyried effeithiau economaidd neu gymdeithasol sylweddol; a/neu

b. effaith sylweddol ar ddiogelwch gwladol, amddiffyn gwladol neu weithrediad y wladwriaeth.

Sganio'r gorwel – archwiliad systematig o wybodaeth i ganfod bygythiadau, risgiau, materion sy'n dod i'r amlwg a chyfleoedd. Mae'n caniatáu paratoi'n well ac ymgorffori mesurau lliniaru yn y broses o lunio polisïau.

System Annibynnol – casgliad o rwydweithiau IP lle mae'r llwybro dan reolaeth endid neu barth penodol.

System Rheoli Diwydiannol (ICS) – system wybodaeth sy'n cael ei defnyddio i reoli prosesau diwydiannol, fel gweithgynhyrchu, trin cynnyrch, cynhyrchu a dosbarthu, neu i reoli asedau seilwaith.

Technolegau cwantwm – Mae technoleg cwantwm yn dibynnu ar egwyddorion ffiseg cwantwm. Mae'r ddealltwriaeth gynyddol a'r rheolaeth o'r hyn a elwir yn 'effeithiau cwantwm' yn arwain at don newydd o ddatblygiadau a fydd yn sail i'n heconomi a'n cymdeithas: synhwyro, trosglwyddo data ac amgryptio, amseru a chyfrifiadura.

Technolegau Gweithredol (OT) – cyfuno caledwedd a meddalwedd i fonitro, rheoli ac awtomeiddio prosesau ffisegol, yn enwedig mewn sectorau diwydiannol fel ynni, gweithgynhyrchu, dŵr a thrafnidiaeth.

Technoleg Cadwyn Atal – ffordd benodol o storio data. Mae cadwyn atal yn enghraifft o gofnodi dosbarthedig – math o dechnoleg storio lle mae dim ond modd atodi ac na ellir tarfu ag ef.

Torri diogelwch data – symud neu ddatgelu gwybodaeth ar rwydwaith heb ganiatâd i barti nad yw wedi'i awdurdodi i gael mynediad at y wybodaeth, na'i gweld.

Uniondeb – ym maes diogelwch gwybodaeth, mae uniondeb yn golygu nad yw gwybodaeth wedi cael ei newid yn ddamweiniol, nac yn fwriadol, a'i bod yn gywir ac yn gyflawn.

Y Ganolfan Seiberddiogelwch Genedlaethol (NCSC) – awdurdod technegol y DU ar gyfer bygythiadau seiber, gan ddarparu ymateb cenedlaethol unedig i ddigwyddiadau seiber er mwyn lleihau niwed, helpu gydag adferiad a dysgu gwersi ar gyfer y dyfodol.

Ymateb i ddigwyddiadau – y gweithgareddau sy'n mynd i'r afael ag effeithiau uniongyrchol tymor byr digwyddiad, a allai hefyd gefnogi adferiad tymor byr.

Ymosodiad Seiber – camfanteisio'n fwriadol ar systemau cyfrifiadurol, rhwydweithiau a sefydliadau sy'n dibynnu ar dechnoleg ddigidol i achosi niwed.

Y rhyngrwyd pethau – yr holl ddyfeisiau, cerbydau, adeiladau ac eitemau eraill sydd wedi'u plannu gydag electroneg, meddalwedd a synwyryddion sy'n cyfathrebu ac yn cyfnewid data dros y rhyngrwyd.