

Onderzoek verstoring plaats- en tijdbepaling

Samenvatting eindrapport

CGI



s[&t

Inhoudsopgave

1	Achtergrond	Fout! Bladwijzer niet gedefinieerd.
2	PNT kennisportaal	4
2.1	Masterclasses	5
2.2	Weerbaarheidsbeoordeling	6
2.3	Mitigatieplan en strategie.....	6
2.4	Nieuws	6
3	GNSS monitoringonderzoek.....	7
4	Conclusies.....	8
5	Aanbevelingen	9

1 Inleiding

Global Navigation Satellite Systems (GNSS); we zijn er allemaal van afhankelijk

Betrouwbare Positie, Navigatie en Tijd (PNT) informatie is van belang voor het goed functioneren van vitale infrastructuren. Het verkrijgen van PNT data gebeurt vaak door middel van een satellietnavigatiesysteem (GNSS), bijvoorbeeld het Europese Galileo of het Amerikaanse GPS. GNSS wordt wereldwijd gebruikt, omdat het zorgt voor nauwkeurige en accurate PNT-data, gratis is te gebruiken en over het algemeen als betrouwbaar wordt ervaren. Toepassingen zoals navigatie van (autonoom) autoverkeer, scheepsvaart en luchtvaart, tijdssynchronisatie voor elektriciteitsdistributie, computer en communicatienetwerken, betalingstransacties en nog veel meer, zijn allemaal afhankelijk van toegang tot GNSS. Het is zo naadloos geïntegreerd in ons dagelijks leven dat soms vergeten wordt hoe afhankelijk de maatschappij van deze informatiebron is en wat het effect zou zijn wanneer de GNSS-signalen worden verstoord.

Vanwege de toenemende afhankelijkheid kunnen verstoringen van de GNSS-signalen steeds meer gevolgen hebben. PNT-bepaling met behulp van GNSS is daarom in 2017 aangewezen als vitaal proces in Nederland. De GNSS-signalen zijn relatief zwak wanneer deze op aarde aankomen en zijn daarom gevoelig voor verstoringen. GNSS-verstoring kan zowel opzettelijk als onopzettelijk plaatsvinden, evenals systematisch of willekeurig. De soorten verstoringen zijn ook wel bekend als jamming en spoofing. De jamming signalen zijn zo krachtig dat de ontvangst van deze signalen het GNSS-signaal van de satelliet overstemt en locatie en tijd niet correct kunnen worden bepaald. Bij spoofing worden de GNSS-ontvangers misleid met foutieve signalen (de spoofing signalen) die het echte satelliet signaal nabootsen. Gespoofde signalen zijn bijna niet van echt te onderscheiden en zodanig opgezet dat een ontvanger locatie- en tijdbepalingen zal blijven doen op basis van deze foute informatie zonder alarm te slaan (er is een parallel met deep fake).

In het eerder uitgevoerde onderzoek "Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie" (IKUS-II)¹ is, heeft het ministerie van Infrastructuur en Waterstaat vastgesteld dat het besef van en de kennis over de kwetsbaarheden van GNSS bij gebruikers moet verbeteren, net als de weerbaarheid van de systemen zelf. Het voorliggende rapport is een vervolgactiviteit van IKUS II.

Hierin is een digitaal informatieportaal ingericht met instrumenten waarmee PNT-gebruikers de kwetsbaarheid van hun systemen kunnen inschatten. Daarnaast is onderzocht welke technologische voorzieningen in nationale of Europese context ontwikkeld kunnen worden om de kwaliteit van het PNT-signaal te monitoren en PNT-gebruikers te waarschuwen wanneer deze kwaliteit onvoldoende is.

Dit project is in opdracht van het ministerie van Infrastructuur en Waterstaat uitgevoerd onder auspiciën van de Europese ruimtevaartorganisatie ESA (het zogenoemde NAVISP EL3 programma) ter ondersteuning van de nationale doelstellingen van de NCTV over weerbaarheid van vitale processen². Het project is uitgevoerd in nauwe samenwerking met ESA, het ministerie van Infrastructuur en Waterstaat, het Netherlands Space Office en het projectteam bestaande uit CGI, NLR en S&T, gezamenlijk onder de noemer GNSS Centre of Excellence. De begeleidende commissie bestaat uit meerdere vertegenwoordigers van de ministeries en (vitale) infrastructuren, voorgezeten door het Ministerie van Infrastructuur en Waterstaat. Deze commissie heeft tijdens en na de uitvoering feedback verzorgd op het project.

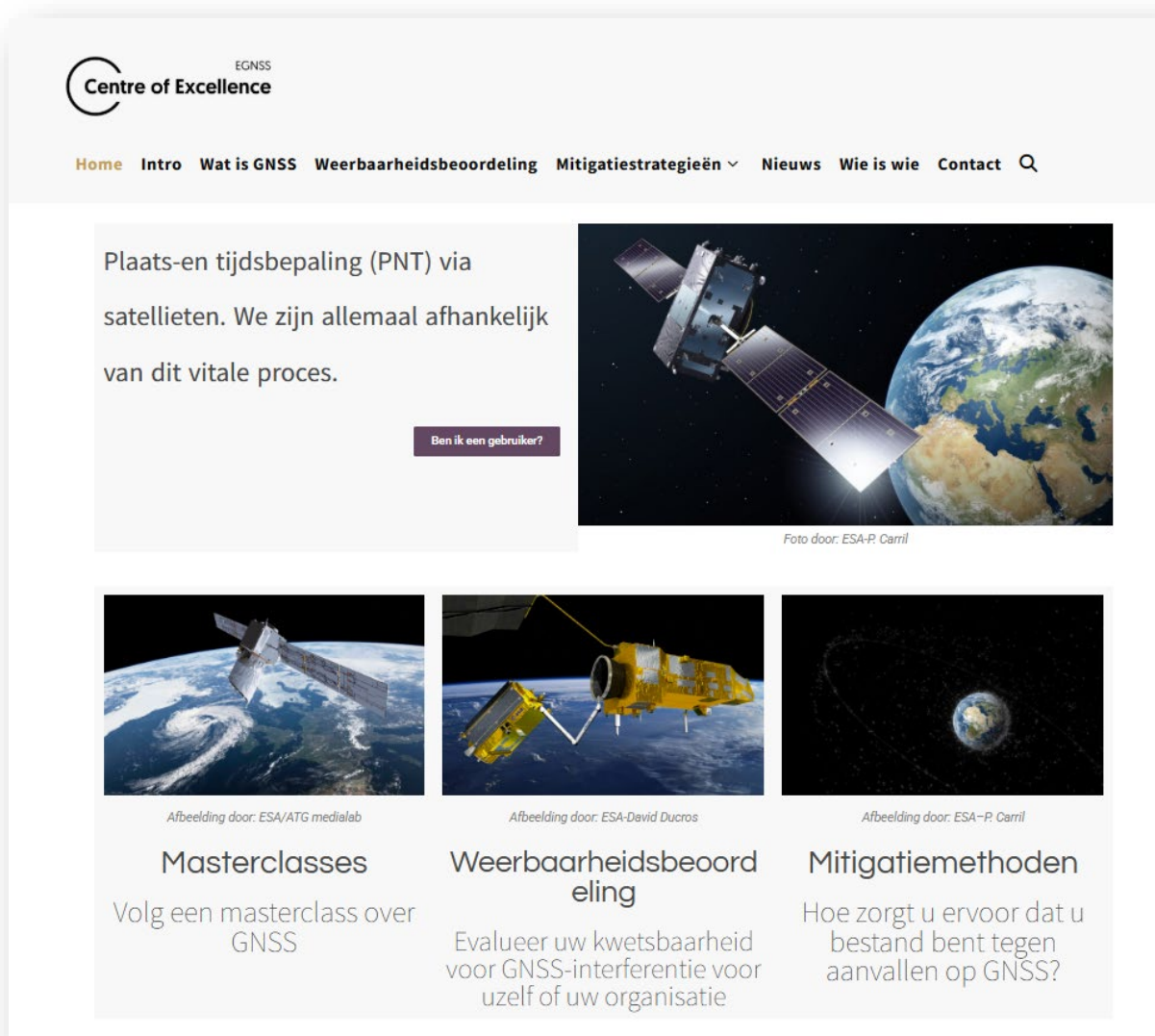
¹ [Kamerstuk II 2022-2033, 24446, nr. 83 Ruimtevaartbeleid](#)

² [Overzicht vitale processen | Vitale infrastructuur | Nationaal Coördinator Terrorismebestrijding en Veiligheid](#)

2 PNT-informatieportaal

PNTportal.eu is een digitaal beschikbaar informatieportaal dat gecentraliseerde toegang biedt tot GNSS-expertise en informatie. Het portaal is bedoeld om (vitale) infrastructuur op het gebied van PNT bij organisaties en individuele personen te ondersteunen.

Het informatieportaal bestaat uit verschillende onderdelen die hieronder worden toegelicht. Alle informatie is beschikbaar in het Engels en het Nederlands. Het informatieportaal is te vinden via de volgende URL link: <https://pntportal.eu/>.



Figuur 1: Voorpagina PNTportal.eu

Het informatieportaal bevat de volgende onderdelen:

- **Introductie:** introductie in GNSS en type toepassingen die GNSS gebruiken.
- **Wat is GNSS:** 10 GNSS Masterclass colleges over specifieke onderwerpen binnen GNSS. Het doel van de colleges is om GNSS-gebruikers te informeren over de verschillende aspecten en achtergrondinformatie van GNSS.
- **Weerbaarheidsbeoordeling:** De tool helpt GNSS-gebruikers met de beoordeling van het weerbaarheidsniveau van hun organisaties tegen GNSS-verstoringen of uitval. De zelfbeoordeling draagt ook bij aan een beter begrip van de systemen die van het GNSS-signaal gebruik maken.
- **Mitigatiestrategieën:** dit onderdeel biedt organisaties advies om het weerbaarheidsniveau van hun systemen te verbeteren. Aangezien elk systeem anders is, zijn de tips die hier te vinden zijn niet gefocust op de technische aspecten van de mitigatie strategieën, maar bieden een algemene opzet om een actieplan op te zetten.
- **Nieuws:** publicatie van (internationaal) nieuws omtrent GNSS en daaraan gerelateerde gebeurtenissen.
- **Wie is wie:** introduceert de organisaties die betrokken zijn bij de ontwikkeling van het portaal.
- **Contact:** contactgegevens voor vragen, feedback of een trainingsaanvraag.

2.1 Masterclasses

Tijdens IKUS-II zijn meer fysieke masterclasses georganiseerd. Deze masterclasses zijn goed ontvangen door de deelnemers. Het is waardevol bevonden om door te gaan met het delen van kennis. Omdat fysieke masterclasses alleen op vaste momenten kennis overbrengen, is er behoefte aan een nieuwe vorm waarbij de doelgroep on-demand toegang heeft tot de informatie. Het resultaat hiervan is de ontwikkeling van een onlineversie van de masterclasses: een serie van korte videocolleges met elk een apart onderwerp. De onderwerpen per masterclass zijn als volgt:

1. Introductie Positie Timing en Navigatie services
2. Basisprincipes van GNSS
3. GNSS-signalen
4. GNSS-ontvangers
5. Fouten en onzekerheden
6. Constellaties en services
7. GNSS-augmentaties
8. Kwetsbaarheden
9. Mitigatie
10. Timing

2.2 Weerbaarheidsbeoordeling

De weerbaarheidsbeoordeling is een tool om gebruikers te helpen de robuustheid van hun systemen te testen als er verstoringen zijn. De testvragen dienen tevens als instrument om eigen systemen beter te begrijpen en een houvast te bieden in het nagaan welke hard- en software wordt gebruikt voor PNT-bepaling. De masterclasses en andere hulpmiddelen moeten ervoor zorgen dat non-experts ook weten waar ze moeten beginnen en weten welke vragen ze moeten stellen om de toetsing te doen. De vragen laten verschillende probleemstellingen zien die zich in een PNT-systeem kunnen voordoen: van onopzettelijk (uitval van de energiebron, verkeerde ontvanger instellingen, willekeurige interferentie) tot opzettelijk (jamming/spoofing, en cyberattacks). Door het systeem én de tekortkomingen te kennen kunnen gebruikers hun systemen beter beoordelen op hun weerbaarheid. Elk weerbaarheidsniveau vraagt om een nieuwe set eisen waar het PNT-systeem aan moet voldoen en toetst door middel van kritische vragen of aan deze eisen daadwerkelijk wordt voldaan. De vragen zijn verdeeld in de volgende onderwerpen: algemene informatie, verberging, limiteren, controleren, isoleren, mitigatie en herstellen. De inspiratie van de inhoud van de tool is gebaseerd op het weerbaarheidsframework van de VS.³

2.3 Mitigatiestrategieën

In het mitigatiestrategie-onderdeel staat een aantal handvatten om een strategie te kiezen die de weerbaarheid van een systeem kan verbeteren. Elk systeem is anders, waardoor de adviezen op deze pagina niet de focus leggen op de technische aspecten van een mitigatiestrategie, maar voornamelijk een kader aanbieden om een algemeen plan van aanpak op te zetten.

Diverse acties kunnen worden uitgevoerd om een systeem weerbaarder te maken. De eerste sectie geeft algemeen advies, zoals bewustwording vergroten en het nemen van fysieke maatregelen.

Het onderhouds-onderdeel bevat een gedetailleerde lijst taken die ervoor zorgen dat soft- én hardware elementen up-to-date blijven en goed blijven functioneren. Het redundantie-onderdeel introduceert manieren waarin de redundantie van een PNT-systeem kan worden vergroot, zodat er in geval van een onderbreking een back-up systeem beschikbaar is. Het beveiligings-onderdeel beschrijft de methodes om zowel de fysieke als de digitale veiligheid van een systeem te vergroten. Bij het upgrades- onderdeel wordt beschreven hoe een systeem dat al goed onderhouden wordt, up-to-date kan blijven. Het laatste onderdeel verwijst naar verdere informatie dat niet in het informatieportaal is opgenomen.

2.4 Nieuws

Op de nieuwspagina worden artikelen met relevantie tot GNSS geplaatst. Elk artikel is een samenvatting van het nieuws en bevat een link naar de originele bron.

³ https://www.dhs.gov/sites/default/files/publications/2020_12_resilient_pnt_conformance_framework.pdf

3 GNSS-monitoringonderzoek

GNSS kan zowel bewust als per ongeluk worden verstoord en beiden zijn een steeds groter wordend risico. Het is van groot belang dat de kennis en het bewustzijn van GNSS-kwetsbaarheden en de hiermee gepaard gaande potentiële risico's, worden vergroot. Het uitgevoerde monitoringonderzoek is bedoeld om praktische ervaring op te doen met het monitoren van GNSS-verstoringen bij vitale infrastructuur in Nederland.

De deelnemende organisaties zijn Stedin-Group, VSL (Nationaal Metrologisch Instituut), luchthaven Schiphol en het Havenbedrijf Rotterdam. Het doel van deze activiteit was om bij de deelnemende organisaties de bewustwording van hun GNSS-gebruik te vergroten. Verder is onderzocht welke technologische voorzieningen in nationale of Europese context ontwikkeld (kunnen) worden om de kwaliteit van het PNT-sigitaal te monitoren en PNT-gebruikers te waarschuwen wanneer deze kwaliteit onvoldoende is. Daarnaast is ervaring opgedaan met interferentiemonitoring bij organisaties op locatie en zijn systeeminstallaties uitgevoerd onder variërende omstandigheden. De gebruikte systemen verschilden in functionaliteit, kosten en gebruikersgemak.

Waarnemingen

Op twee van de vier locaties werden zogenoemde Radio Frequency Interference (RFI) verstoringen gedetecteerd door de monitoringsystemen. Gedurende de testen zijn honderden versturende signalen waargenomen, waarvan er 54 zijn geclassificeerd als een waarschuwing en 23 als een alarm (ZIE TABEL). Het kenmerk van een waarschuwing is dat het verstoorde signaal korter duurt dan 30 seconden en een laag vermogen heeft. Een alarm wordt gekenmerkt door een hoger vermogen en/of langere tijdspanne. De als waarschuwing en alarm gekenmerkte waarnemingen kunnen in potentie een versturend effect hebben.

Tijdens het onderzoek is met name gemonitord in de L1-frequentieband. De L1-signalen zijn vrijwel altijd de basis voor navigatie en tijdbepaling. Tijdens het onderzoek werden lange (30 seconden of meer) en korte (1 seconde durende) verstoringen waargenomen in de buurt van snelwegen. De impact van deze verstoringen is tot dusver onbekend omdat de monitoringapparatuur niet verbonden was aan de systemen van deelnemende organisaties. Ook is er gekeken naar de L5-frequentieband. Deze L5-band wordt met name gebruikt in de luchtvaart. Wanneer een positiebepaling wordt gedaan met minder satellieten kan dat ook zorgen voor een mindere kwaliteit van het GNSS-sigitaal. Dit is ook waargenomen tijdens de testen.

Een opmerkelijk resultaat was op een locatie waarbij de locatie en de kracht van het interferentiesigitaal nagenoeg constant bleken. Deze verstoring bleek uit de omgevingsapparatuur van de organisatie zelf te komen. Hiermee werd inzichtelijk dat systemen van organisaties zelf ook onbewust een versturend effect kunnen hebben op het GNSS-sigitaal. Welk effect de verstoringen hadden op de omgeving is niet onderzocht, wel zijn de bronnen van de verstoringen te achterhalen.

Locatie	Aantal waarschuwing-verstoringen	Aantal alarm-verstoringen
1	9	0
2	14*	15
3	8	0
4	23*	8*

*de constante verstoringen die ontstonden door de omgevingsapparatuur van de organisatie zelf zijn geteld als één waarneming.

4 Conclusies

PNT kennisportaal

Voor de organisaties die verantwoordelijk zijn voor vitale infrastructuur en processen, is bewustzijn over het veilig en verantwoord gebruik van GNSS informatie een eerste stap in het realiseren van een handelingsperspectief. Tijdens het IKUS-II project kwam naar voren dat het bewustzijn van de afhankelijkheid en de mogelijke effecten niet altijd aanwezig is. Er is daarom besloten hier extra aandacht aan te geven en kennis over dit onderwerp toegankelijk te maken door de ontwikkeling van het kennisportaal.

Met de feedback van de begeleidingscommissie is het kennisportaal gedurende het project ontwikkeld en is het 'gelanceerd' middels nieuwsberichten vanuit verschillende organisaties. In een relatief korte tijd heeft het portaal honderden bezoeken gehad.

Interferentiemonitoring

GNSS-interferentie is geen onbekend risico aangezien het al meetbaar én voelbaar is op meerdere plekken in en buiten Europa. De organisaties die deelgenomen hebben aan dit onderzoek hebben actief meegedacht met het selecteren van de meetlocaties en zijn geïnformeerd over de resultaten.

Een monitoringsysteem geeft meldingen bij waarnemingen van verminderde GNSS-kwaliteit waarmee een organisatie inzicht krijgt en conclusies kan trekken over de impact ervan. Met deze informatie kan de organisatie mitigerende maatregelen nemen tegen de impact van verstoring van het GNSS-signaal. In samenwerking met de vier deelnemende organisaties zijn meerdere aandachtspunten geïdentificeerd voor het installeren van een monitoringssysteem. Niet alle, voorafgaand geïdentificeerde locaties, bleken geschikt voor de monitoring, omdat niet werd voldaan aan vier criteria. De uiteindelijke locaties werden gekozen op basis van: 1) de locatie is van belang voor de organisatie, 2) er is stroom aanwezig, 3) apparatuur kan afgeschermd worden opgeslagen en 4) de ontvanger wordt niet gehinderd door objecten (Line of Sight (LOS)). Na de selectie op basis van de criteria zijn voortesten uitgevoerd om de correcte verwerking te bevestigen.

In een relatief korte tijd zijn er honderden verstoringen waarnemingen gedaan waarvan er 77 werden geclassificeerd als waarschuwing of alarm (zie hoofdstuk 3). De monitoringsystemen hadden geen directe verbinding met de operationele systemen van de deelnemende organisaties waardoor eventuele gevolgen van de verstoring niet meetbaar waren.

Het onderzoek laat echter wel zien dat er verstoringen in het GNSS-spectrum meetbaar zijn. Door de kracht van verstoringen te vergroten, wat een relatief eenvoudige stap is, kan de verstoring toenemen in impact en neemt ook de omvang van het gebied waar de verstoring wordt gemeten, toe. Het is bijvoorbeeld bekend in de luchtvaart dat spoofing en jamming op grotere schaal vaker een probleem vormt⁴. Alle organisaties die afhankelijk zijn van GNSS moeten rekening houden met deze ontwikkeling.

⁴ [Piloten en politici bezorgd om verstoring GPS-signaal luchtvaart](#)

5 Aanbevelingen

IKUS-II

Gezien de technologische complexiteit van GNSS en de mogelijke impact van GNSS-verstoringen zijn de aanbevelingen uit IKUS-II nog steeds relevant. Deze aanbevelingen kunnen [hier](#) worden gevonden.

PNT-informatieportaal

Het openbaar beschikbaar maken van kennis en expertise helpt organisaties bij de bewustwording van de kwetsbaarheden in de toepassing van PNT. Het wordt aanbevolen om het informatieportaal blijvend onder de aandacht te brengen. Daarnaast moet de content van het portaal up-to-date gehouden worden zodat het informatieportaal relevant blijft.

Interferentiemonitoring

Ondanks dat de geregistreerde waarnemingen tijdens het veldonderzoek beperkt vermogen hadden, kunnen spoofing- en jamming-aanvallen worden uitgevoerd met meer vermogen. Er moet rekening gehouden worden met aanvallen die specifiek gericht zijn op Nederlandse vitale infrastructuur. Dit kan veel schade aanrichten en vitale processen hinderen. De volgende aanbevelingen worden gedaan:

- Breng bewust GNSS-gebruik blijvend onder de aandacht (aanbeveling aan de overheid)
- Overweeg om interferentiemonitoringsystemen te implementeren om waarschuwingen te ontvangen. Interferentiemonitoringsystemen kunnen (vitale) organisaties informeren wanneer er waarnemingen zijn van verstoringen, waarmee organisaties kunnen bepalen hoe te handelen (aanbeveling aan de overheid en vitale infrastructuur organisatie).
- Organisaties die verantwoordelijk zijn voor vitale processen of infrastructuur die gebruik maken van PNT, wordt aangeraden een actieplan beschikbaar te hebben voor het geval PNT uitvalt (aanbeveling aan verantwoordelijken voor vitale processen en infrastructuur)

Interferentiemonitoringstrategie

Door het monitoren van verstoringen van de GNSS-signalen bij (vitale) processen en infrastructuren, kunnen organisaties gewaarschuwd worden wanneer de GNSS-signalen verstoord worden en daarmee bepalen of en welke acties genomen moeten worden. Het is belangrijk te noemen dat niet alle GNSS-verstoringen direct omvangrijke effecten hebben. Het effect van de verstoring is namelijk erg afhankelijk van de aard en kracht van de verstoring en de mate waarin de verstoorde toepassing kritisch of essentieel is. Bij het implementeren van interferentiemonitoring is het volgende van belang:

- Wees op de hoogte van de regelgeving omtrent interferentiemonitoring
- Definieer de waarschuwing- en alarmwaardes die voor eigen organisatie relevant zijn. Eisen voor integriteit, nauwkeurigheid en continuïteit van de PNT-signalen variëren per toepassing.
- Bepaal wie toegang tot deze data krijgt en definieer ook wat de organisatie met de monitoringdata mag doen.
- Een netwerk van monitoringsystemen kan zorgen voor een bredere dekking en meer inzicht dan één systeem.
- Coördineer met nationaal belanghebbende partijen het opzetten van een netwerk van monitoringsystemen.
- Stel een actieplan op voor wanneer interferentie plaatsvindt en stel een mitigatiestrategie op. Bijvoorbeeld door gebruik te maken van state-of-the-art apparatuur, beveiligde signalen zoals Galileo PRS in te zetten of een combinatie van bronnen in te zetten.

Relatie tot de Cyberbeveiligingswet

De Europese Unie heeft de Netwerk en Informatie Beveiligingsrichtlijn (NIS2) ontwikkeld om digitale en economische weerbaarheid te vergroten. In Nederland is NIS2 geïmplementeerd in de vorm van de cyberbeveiligingswet (Cbw).

Het wordt aanbevolen aan de overheid om te onderzoeken of kwetsbaarheden als gevolg van GNSS-afhankelijkheden in wettelijke kaders kunnen worden opgenomen zodat (vitale) organisaties nadrukkelijk aangezet worden tot het vergroten van hun weerbaarheid.

Frequentie van IKUS onderzoek

In IKUSII is geconstateerd dat het bewustzijn over de kwetsbaarheid van (vitale) processen en infrastructuur voor de uitval van PNT, bij diverse organisaties en sectoren die verantwoordelijk zijn voor die infrastructuur en processen ontbreekt of beperkt is. Dit staat in groot contrast tot de potentiële gevolgen die verstoring en uitval van PNT kan hebben voor de Nederlandse samenleving. Het is aan te bevelen met enige regelmaat opnieuw het bewustzijn te onderzoeken om een indruk te krijgen of de weerbaarheid tegen uitval van PNT toeneemt.