Twitter Thread by Security Analyst @ SRSRM



Security Analyst @ SRSRM
@Selyst



@tazwake @DanielGDresner @ciaranmartinoxf @Tob1Leron @TheEPS1 1/ x Cc @DuncanChapple Long intake of breath as I realise I have recently started the wrong MSc....
@aj66inuk and I have been discussing that whilst the world has changed, some things have not. #Sabotage is an outdated concept unless you think that Cyber is an extension..

@guyyeomans @tazwake @DanielGDresner @ciaranmartinoxf @Tob1Leron @TheEPS1 @DuncanChapple @aj66inuk 2/x an extension of what our former Cold War adversaries were trying to do to us. In 1982 Duncan Campbell spelled out where adversaries would try to attack us. But with Glasnost this became unfashionable and apparently unaffordable.
https://t.co/CLLiVxTbXW

@guyyeomans @tazwake @DanielGDresner @ciaranmartinoxf @Tob1Leron @TheEPS1 @DuncanChapple @aj66inuk 3/X Defector information in the public domain gave us some insights was to what the Warsaw Pact threat to our CNI might look like. Discussions with former adversaries, now Polish, (East) German and Czech allies wld be informative here.

@guyyeomans @tazwake @DanielGDresner @ciaranmartinoxf @Tob1Leron @TheEPS1 @DuncanChapple @aj66inuk 4/X Believing there is a credible threat has always been our challenge here in UK. Understanding how a nation state adversary would come at us would be the next step.
It will be persistent, an adversary like the GRU will have been analysing our CNI for over 70 years

@guyyeomans @tazwake @DanielGDresner @ciaranmartinoxf @Tob1Leron @TheEPS1 @DuncanChapple @aj66inuk 5/x They will have formed physical and logical plans to attack us. It some cases they may know our assets and our vulnerabilities better than we do. CARVER Shock is an old-school tool that gives an idea how they will come after us. You can apply it....
https://t.co/RIo3UjPghU

@guyyeomans @tazwake @DanielGDresner @ciaranmartinoxf @Tob1Leron @TheEPS1 @DuncanChapple @aj66inuk 6 / x ... at a national level, or at a tactical level to look at a single system or site. Dont forget a nation state try to make a Sabotage attack look, deniable: like an accident, or script kiddies or organised crime

@guyyeomans @tazwake @DanielGDresner @ciaranmartinoxf @Tob1Leron @TheEPS1 @DuncanChapple @aj66inuk 7/x One you have believed in and understood the threat, then you can look back from the defender's perspective and look at where you may be vulnerable.
Thats where the BIA begins. @TheBCEye is a great place to start.

@guyyeomans @tazwake @DanielGDresner @ciaranmartinoxf @Tob1Leron @TheEPS1 @DuncanChapple @aj66inuk @TheBCEye 8/ X Withdrawn some years back CESG's business impact level tables (long withdrawn) would be a great place to start to identify your assets. Thanks to @DegaussersEU for keeping them on-line here https://t.co/tR6zLZjWhO

@guyyeomans @tazwake @DanielGDresner @ciaranmartinoxf @Tob1Leron @TheEPS1 @DuncanChapple @aj66inuk @TheBCEye @DegaussersEU 9/x Not only is your threat dynamic, so is your infrastructure and your business needs. For instance our pharma supply chain will be more important in 2021 than it was in 2019 and needs to be reviewed accordingly. Little of UK's CNI sits inside government....the secret sauce

@guyyeomans @tazwake @DanielGDresner @ciaranmartinoxf @Tob1Leron @TheEPS1 @DuncanChapple @aj66inuk @TheBCEye @DegaussersEU 10/10 the secret sauce is being able to recognise the needs of business AND the needs of the nation and show where they can overlap. Applying BS11000 / ISO 44001 would be the ideal way of working together https://t.co/6w1neRDavz

@guyyeomans @tazwake @DanielGDresner @ciaranmartinoxf @Tob1Leron @TheEPS1 @DuncanChapple @aj66inuk @TheBCEye @DegaussersEU 11/ X A final reflective point. At 6/X above I mention that in order to obfuscate attribution in this #GreyZone , a professional saboteur will try to disguise their attack to look like an accidental or criminal criminal act..... 12/ X

@guyyeomans @tazwake @DanielGDresner @ciaranmartinoxf @Tob1Leron @TheEPS1 @DuncanChapple @aj66inuk @TheBCEye @DegaussersEU 12/ X As opposed to looking at a single risk, our protection philosophy was based on helping CNI protect against a broad range of threats:- "Disruptive Challenges" as per para 1.5 of Dealing with Disaster, from CCS in @cabinetofficeuk 3rd edition here:
https://t.co/8dFM1dzT7k

@guyyeomans @tazwake @DanielGDresner @ciaranmartinoxf @Tob1Leron @TheEPS1 @DuncanChapple @aj66inuk @TheBCEye @DegaussersEU @cabinetofficeuk 13/ X Taking this broad risk approach allowed us to demonstrate alignment with Integrated Contingency Planning and Integrated Emergency Management.

Some may remember the great storms of 1987..... ?

@guyyeomans @tazwake @DanielGDresner @ciaranmartinoxf @Tob1Leron @TheEPS1 @DuncanChapple @aj66inuk @TheBCEye @DegaussersEU @cabinetofficeuk 14/ X The only East Coast port that continued to operate throughout and after those storms in 1987 was the one that have invested in our #Resilience recommendations in advance. They recovered their investment in days, matched their 1986 profit in weeks!

https://t.co/mZbrUcgjlv

@guyyeomans @tazwake @DanielGDresner @ciaranmartinoxf @Tob1Leron @TheEPS1 @DuncanChapple @aj66inuk @TheBCEye @DegaussersEU @cabinetofficeuk // the one that HAD invested....