Ja, ik zou op een aantal punten willen reageren. Om te beginnen zou ik willen zeggen dat politie en justitie zich niet voor hun werk hoeft te schamen, en geheimhouding zou daarom niet de norm mogen zijn. Geheime politiediensten hebben het risico te ontsporen zoals de octopus- en IRT-affaire hebben aangetoond. Geheime rechtelijke uitspraken zijn ook gevaarlijk zoals "rubber-stamp-FISA" in Amerika zeer recentelijk heeft aangetoond. Mijn voornaamste kritiekpunten zijn dan ook over de stiekeme sfeer die het hele voorstel ademt.

Ik zal de volgorde van de toelichting aanhouden.
2. Onderzoek in een geautomatiseerd werk
Er zijn in de voorstellen voor het "terughacken" niet voldoende garanties dat deze bevoegdheid niet misbruikt zal worden. De verdachte zal, als de zaak nooit voor de rechter komt, niet te weten komen dat hij bespioneerd is, en heeft dus nooit de mogelijkheid om verhaal te halen over de rechtelijke toets. Een proces waar maar een van de partijen het woord kan doen is niet echt eerlijk. Er zijn argumenten waarom mensen niet op voorhand ingelicht worden van het onderzoek tegen hun persoon, maar op het moment dat iemand redelijkerwijs geen verdachte meer is vervallen die. Op dat moment moet de ex-verdachte op de hoogte gesteld worden omdat de rechtspraak in principe openbaar is.

Daarmee samenhangend: De gevonden gegevens zijn mogelijk ontlastend voor de verdachte, en zouden daarom in zijn geheel tot de beschikking moeten staan van de verdachte zodra deze op enig moment voor de rechter staat (In het kader van PRISM heeft al iemand die van een misdaad verdacht werd, zijn NSA-gegevens opgevraagd in Amerika, omdat die volgens hem aantonen dat hij onschuldig is).

Een derde reden dat de verdachte in ieder geval van de hack-activiteiten moet weten, is dat hij zijn private sleutels zal moeten vervangen. Deze zijn namelijk bekend geworden bij de onderzoekers, terwijl absolute geheimhouding de norm is.

3. De ontoegankelijkmaking van gegevens
Gezien de vaak bedrijfscritische processen die zich op het internet afspelen, zou er een duidelijke mogelijkheid tot verweer moeten zijn voordat er gegevens ontoegankelijk gemaakt worden. Dit zou zeer vlot moeten gebeuren. Ik zou dan ook zeggen dat de gegevens op verzoek van de verantwoordelijke binnen een paar uur weer on-line gezet zouden moeten kunnen worden. Een paar uur is voldoende om de directe schade in te perken, en het mogelijke legale gebruik van de gegevens kan meestal niet uitgesloten worden (zelfs de techniek van virussen en botnets is vaak erg interessant voor informatici).

4. Het decryptiebevel aan de verdachte

Zoals al eerder genoemd, is de veiligheid van computersystemen gebaat bij absolute geheimhouding van bijvoorbeeld prive-sleutels. Het decriptie-bevel zorgt dat het gebruik hiervan een straf van 3 jaar kan opleveren als je een wachtwoord kwijt bent. Voor de computer security in Nederland zou het gebruik van encryptie juist bevorderd moeten worden.

5. De heling van gegevens

Het lijkt mij onmogelijk om gegevens op hun herkomst te beoordelen. Strikt genomen, wordt volgens dit voorstel de originele producent strafbaar als zijn gegevens door een misdrijf gekopiëerd zijn, aangezien hij zelf ook over gegevens beschikt die door een misdrijf zijn verkregen (door de hacker).

Het argument dat "gestolen" informatie gedeeld mag worden in het algemeen belang is niet sluitend. Het algemeen belang kan in veel gevallen betwist worden, en als de informatie dan al in de krant staat zou plotseling iedereen crimineel zijn. Als de rechter zou beoordelen dat Edward Snowden niet in het algemeen belang gehandeld heeft, zou de halve wereldbevolking volgens deze wet vervolgd kunnen worden.

Maar naast deze logische exercities is er nog een principiëler bezwaar, namelijk dat deze wet het hebben van bepaalde gegevens strafbaar stelt, wat het begin vormt van censuur. Omdat niemand de gegevens mag hebben, kan ook niet meer beoordeeld worden, of het terecht is dat ze niet gedeeld mogen worden.