

Interrogazione

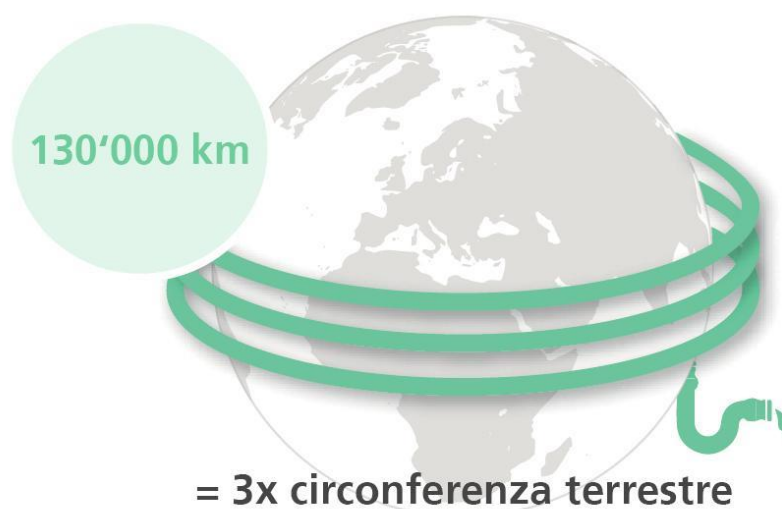
Quale sicurezza idrica?

Onorevole Signor Sindaco,
Onorevoli Signori Municipalì,

L'acqua è una risorsa vitale che con il tempo sarà destinata a rivestire un'importanza sempre più rilevante non soltanto da un punto di vista concreto, ma anche come strumento di forza all'interno dei rapporti e delle relazioni tra gli Stati.

Un'importanza così ampia è testimoniata dal fatto che l'acqua oggi viene chiamata l'oro blu e a ragione, dal momento che il nostro corpo è composto principalmente da acqua, e senza la quale nessuna forma di vita sulla terra potrebbe sopravvivere a lungo. L'acqua è la principale fonte di vita dell'umanità e si sta trasformando in una risorsa strategica vitale a causa della sua rarità che ne fa aumentare in modo esponenziale il valore e il potere a livello politico e internazionale.

L'acqua diventerà il nuovo petrolio nel futuro, la nuova ricchezza che porterà le nazioni a combattersi per averne l'accesso e il controllo, nuovo punto focale della politica e anche dell'economia. Solo in Svizzera, la rete idrica misura 130'000 km pari a 3 volte la circonferenza terrestre.

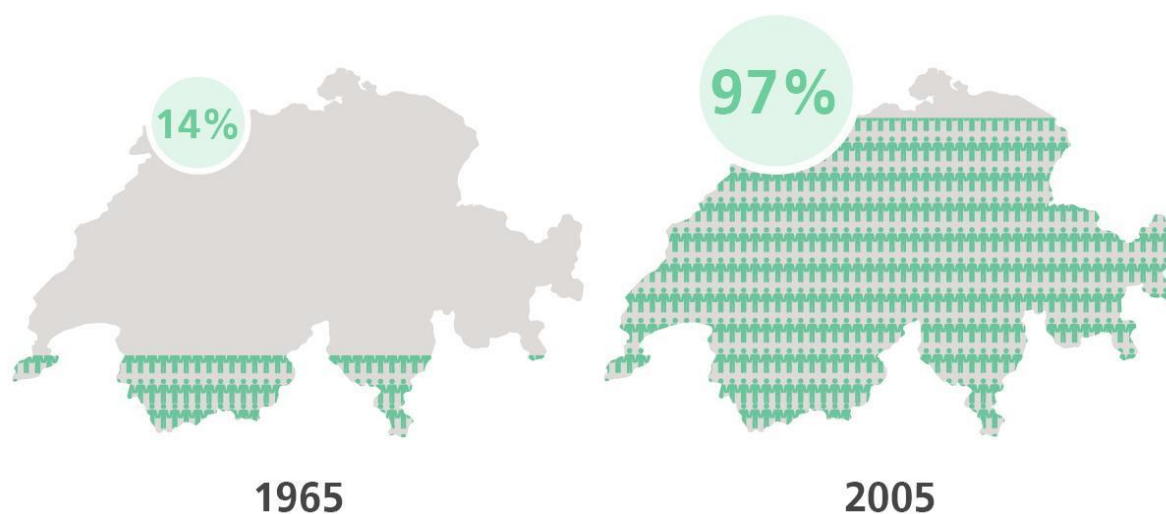


Recentemente sono venuti alla luce gravissimi attacchi hacker alla rete informatica, nel mirino, infatti, sono già finite grandi banche, compagnie elettriche e società di trasporti,

che hanno ad esempio compromesso il funzionamento di centrali nucleari (Cernobyl) e reti di trasporto (metrò di Kiev). Rosneft, la prima azienda petrolifera Russa, ha visto il suo sito andare in tilt ed è dovuta passare ai sistemi informatici di riserva (non senza imbarazzo da parte della compagnia stessa). Altre società come Bashneft - ora parte di Rosneft dopo l'acquisizione dello scorso anno - Mars e Nivea sono state coinvolte. I danni però sembrano essere stati contenuti, specie al sistema bancario.

Le notizie di contagio, ad ogni modo, si sono moltiplicate e tra le vittime ci sono anche giganti globali come la britannica Wpp (pubblicità) o la danese Maersk (spedizioni). Ora resta da capire se la diffusione del virus sarà capillare come nel caso di WannaCry oppure gli esperti informatici saranno in grado di contenerlo. Un dettaglio fa temere il peggio: secondo Symantec, colosso della cyber-sicurezza, anche Petya (come WannaCry) userebbe EternalBlue, una delle 'armi' trafugate all'NSA (National Security Agency), gli 007 digitali americani. Ovvero un codice d'attacco - in gergo 'exploit'. Nel caso di Wannacry la cyber arma ha sfruttato una vulnerabilità di un software di Microsoft (che poi ha corretto la falla) ed è stata diffusa da un misterioso gruppo di hacker di nome Shadow Brokers, che in qualche modo ha sottratto una serie di strumenti digitali all'agenzia Usa e poi li ha messi in rete.


Fino al 1965 i cittadini svizzeri allacciati a una centrale di depurazione delle acque erano il 14 per cento. Nel 2005 erano diventati il 97 per cento, il che – considerato che il 2 per cento della popolazione è rappresentato da persone che vivono in zone discoste o poco densamente abitate in cui non serve allacciamento – portava già allora il potenziale di sviluppo ancora non sfruttato all'1 per cento. Nel frattempo alla nostra rete di canalizzazioni, lunga ormai oltre 130 000 km, sono collegati 800 impianti di depurazione. E al potenziamento dell'intera opera, **costata 50 miliardi di franchi svizzeri**, ha contribuito la Confederazione con sovvenzioni per un totale di 5,3 miliardi di franchi.




Da allora l'infrastruttura esistente ha dovuto essere mantenuta e sviluppata per far fronte a nuove sfide, tra queste non bisogna dimenticare il cyberspazio (considerando che la rete idrica viene sorvegliata da sistemi informatici) riducendo al minimo il rischio di estremismo online.


Impianti di depurazione moderni e ben equipaggiati, come pure gli impianti di approvvigionamento idrico, con un alto sistema di sicurezza, saranno indispensabili anche in futuro per garantire costantemente acqua pulita e di buona qualità ai nostri cittadini.


Alla luce di quanto esposto sopra, avvalendoci delle facoltà concesse dalla LOC, chiediamo al Lodevole Municipio:


 In che misura la rete idrica di Lugano è dipendente dall'informatica? Quanti sono gli impianti che dipendono direttamente dalla rete internet?


 Esiste un sistema di backup dei dati? Se sì, da chi viene gestito? Quanto il costo di questo servizio?


 Sono mai stati perpetrati attacchi hacker alla rete idrica?


 Quali sono le tempistiche di reazione ad un eventuale attacco informatico alla rete idrica? In caso di blocco dell'approvvigionamento idrico, a seguito di un attacco informatico, è possibile ripristinare l'afflusso d'acqua in tempi brevi (magari con un sistema di rete in "parallelo")? Se no, quanto tempo può durare la "panne"?

 Esiste una squadra d'emergenza per questo tipo di attacco? Se sì, con quale tipo di formazione?

 In che modo viene verificata la professionalità e l'identità di chi è preposto alla sicurezza informatica (e fisica) dell'azienda di distribuzione?

 Esiste un registro un registro dettagliato (dipendenti e non) di chi entra negli acquedotti? Chi ne verifica l'identità e l'eventuale pericolosità?

 Quale tipo di sicurezza è applicato alle entrate "fisiche" degli acquedotti? È sufficiente questo livello di sicurezza?

 Quali e quante misure precauzionali, sulla rete idrica, sono state prese per prevenire qualsiasi tipo di atto terroristico (sia questo informatico o materiale) che possa recare danno alle cose e alle persone? Con quali costi?

In attesa delle Vostre puntuali risposte porgiamo
Distinti Saluti

Sara Beretta Piccoli e Giovanni Albertini (Consiglieri Comunali PPD e GG)